Verbraucherzentrale
Bundesverband

Digital Omnibus: Simplification Yes – Deregulation No

Position by the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv) on the European Commission's Call for Evidence on the Digital Omnibus

10/10/2025

Content

I. Relevance for consumers

Digital rules shape how consumers live, communicate and shop online every day. They determine whether online advertising respects privacy or exploits personal data; whether companies use AI systems to discriminate against consumers or manipulate them or exploit their personal weaknesses; whether devices are secure against misuse; and whether online shops and platforms take real responsibility when something goes wrong. From the protection of personal data and cybersecurity to fair platform practices, these rules define how safe and trustworthy the digital world feels.

Simplifying and aligning the EU's digital rulebook can make digital services more transparent and easier to use. Yet such efforts must reinforce – not weaken – the safeguards that protect consumers against data misuse and unfair practices. Ultimately, the Digital Omnibus must aim to strengthen privacy, safety and trust in the digital environment. Clear, coherent regulation enables people to understand their rights, make informed choices and rely on digital tools that genuinely serve their interests and values. It also provides legal certainty for businesses, allowing them to operate fairly and on a level playing field across the Single Market — a stability that ultimately benefits consumers through safer, more trustworthy and competitive digital services.

II.Summary

From a consumer perspective, the Digital Omnibus should make EU digital rules clearer, more consistent and easier to understand. Consequently, the overarching goal is to create a digital rulebook that strengthens consumer and fundamental rights while improving the clarity and usability of EU digital legislation. To achieve these objectives, the European Commission should consider the following views and positions:

- **Any ePrivacy reform** should streamline the user experience without diluting level of protection of the ePrivacy Directive and the GDPR. The way forward is to reduce structural risks by prohibiting tracking and profiling for advertising, to introduce binding privacy-preserving user signals and to fostering coordinated enforcement.[1] This approach reduces consent noise while strengthening user control and fair competition. Strong rules affirm the EU's role as a global leader and reinforce digital sovereignty. They keep rights at the core of Europe's digital future and uphold the European Commission's commitment to protect its citizens.
- In vzbv's view, the adjustments outlined by the European Commission in the Call for Evidence carry a serious risk of undermining the protection of fundamental rights and should be accompanied by an independent assessment of impacts on fundamental rights.
- The **General Data Protection Regulation (GDPR)** is a proven legal framework and should not be reopened. The European Commission should focus on coherent interpretation and strict enforcement. The EU should strengthen support for SMEs through clear guidance, model clauses and practical tools. Only consistent enforcement and targeted support can safeguard competitiveness, innovation and fundamental rights in the digital age.[2]
- The application of the **Artificial Intelligence Act (AI Act)** should not be delayed (no stop-the-clock), nor should its scope be limited by exemptions or weaker rules for SMEs and mid-caps, or by narrowing the scope of high-risk AI through the deletion of Annex I, the limitation of scope in Annex III, or the weakening of the high-risk AI classification mechanism. Such dilutions would significantly undermine consumer protection by preventing consumers from exercising their rights. As the Digital Omnibus aims to consolidate provisions and reporting and documentation obligations with other digital legal acts, it must weaken the AI Act's provisions that constitute safeguards for consumers. This is particularly important regarding the prohibited AI practices, the core provisions on high-risk AI and GPAI in Chapters 3 and 5, the labelling and transparency obligations, and consumers' right to explanations of high-risk AI decisions.
- **Cybersecurity related incident reporting obligations** must remain robust and timely to ensure that consumers are adequately informed and protected. Simplification should enhance clarity and efficiency without compromising transparency, enforcement, or the rights of consumers in the digital ecosystem. In particular, any streamlining must not come at the expense of the substance, detail or frequency of reporting.

---

[1] These positions and demands are set out in detail in Verbraucherzentrale Bundesverband: Perspectives for the Regulation of Personalised Advertising, 2025, https://www.vzbv.de/sites/default/files/2025-02/25-02-10_Positionpaper_vzbv_Personalised-Advertising.pdf, 01.10.2025.

[2] These positions and demands are set out in detail in dass.: DSGVO: Entlastung ja – Aufweichung nein, 2025, https://www.vzbv.de/sites/default/files/2025-05/25-05-07_Kurzstellungnahme_vzbv_DSGVO-Vereinfachung.pdf, 02.10.2025.

- **Operators of online marketplaces** should take more responsibility when third-party traders infringe EU law. Additional targeted due diligence obligations should be introduced. Responsibility must be supported with accountability: Operators of online marketplaces should be subject to joint and several liability alongside traders for infringements.

III. Introduction

With the Digital Omnibus, the European Commission aims to simplify and harmonise existing digital regulations.[3] However, simplification must not be confused with deregulation. Regulation is not synonymous with bureaucracy, nor does it inherently hinder innovation. On the contrary, clear, coherent rules create legal certainty and foster innovation by establishing predictable frameworks that benefit both businesses and consumers. From a consumer perspective, well-designed legal framework relieves individuals of unnecessary burdens, enhances trust and protects them from opaque practices. Consumers are not passive recipients but an essential part of the European digital economy, whose trust is a precondition for sustainable growth. Simplification can therefore only be welcomed if it enhances clarity and usability without eroding substantive safeguards. The goal must be to make the rulebook more understandable and accessible while preserving – and where necessary strengthening – the protection of consumer and fundamental rights.

The Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv) welcomes the European Commission's continued commitment to improving the coherence and effectiveness of the EU's digital rulebook. This is essential for safeguarding consumers' rights and for ensuring a fair, competitive and trustworthy digital environment. Therefore, vzbv appreciates the opportunity provided by the European Commission to present its views on this important topic.

IV. Positions in detail

1. ePrivacy Reform

The digital advertising ecosystem has developed into a complex network of actors driven to collect personal data with little oversight. Through extensive tracking and profiling, consumers are targeted based on personal preferences and vulnerabilities, creating profound informational and power asymmetries. This undermines privacy, facilitates manipulation and fosters discrimination, leaving

[3] European Commission: Digital Omnibus. Call for Evidence, 2025, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Digital-package-digital-omnibus-_en, 01.10.2025.

many consumers powerless. Studies commissioned by the European Commission confirm these risks.[4] vzbv therefore welcomes that the European Commission intends to modernise the ePrivacy Directive's provisions on protecting users' terminal equipment and on access to and collection of information from such equipment.

Against this backdrop, it is essential to **recall the existing legal baseline**, which sets clear limits on device access and is central for assessing reform proposals: Article 5(3) of the ePrivacy Directive protects the integrity of terminal equipment: storing or accessing information requires prior, informed consent unless strictly necessary for a requested service, regardless of whether personal data are processed. This safeguard applies technology-neutrally (e.g. to cookies, local storage, device and advertising IDs, SDKs, pixels). The Court of Justice of the European Union (CJEU) in Planet49 (C-673/17) confirmed that valid consent must be active and specific. The European Data Protection Board (EDPB) clarified in Guidelines 05/2020 that cookie walls and mere scrolling do not constitute valid consent, and in Guidelines 03/2022 highlighted how dark patterns undermine genuine choice.

Yet existing laws like the General Data Protection Regulation (GDPR), the ePrivacy Directive and related laws struggle to adequately address the systemic risks posed by personalised advertising. The GDPR's flexibility and broad definitions have inadvertently fostered implementation challenges as well as enforcement gaps. The complexity of the advertising ecosystem makes it nearly impossible for consumers to understand how their data are collected and used, while deceptive designs undermine control and consistently nudge users towards acceptance. Sector-specific rule books like the Digital Service Act (DSA), the Regulation on the Transparency and Targeting of Political Advertising (TTPA) or the Artificial Intelligence Act (AIA) offer valuable measures but fall short of establishing comprehensive protections, as their scope is often limited to specific actors or contexts rather than ad-dressing the ecosystem as a whole.

Only stronger limits and meaningful accountability can effectively mitigate the risks of tracking and profiling for advertising in the open internet.

Consumers consistently report high concern about online advertising. The Consumer Conditions Scoreboard (CCS) 2023 shows that 70% of consumers are concerned about how their personal data are used and shared, and 38% reported a decline in their trust in e-commerce for this reason. [5] In a special Eurobarometer on the Digital Decade 2024, 46% stated that misuse of personal data is the most significant personal impact of digital technologies. [6]

Reforms that further normalise tracking and profiling for advertising risk undermining trust in the Single Market. Trust is a precondition for the uptake of digital services and for a resilient internal market. Lowering protection predictably depresses adoption and harms small and medium-sized enterprises (SMEs). Protecting consumers is therefore not only a matter of rights but also a prerequisite for economic resilience and sustainable growth.

---

[4] Armitage, Catherine u. a.: Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers. Study prepared for the European Commission, 2023, https://data.europa.eu/doi/10.2759/294673, 01.10.2025.

[5] European Commission: Consumer Conditions Scoreboard, 2023, S. 20, https://commission.europa.eu/system/files/2023-10/consumer_conditions_scoreboard_2023_v1.1.pdf, 01.10.2025.

[6] Dass.: The Digital Decade. Special Eurobarometer 551, 2024, https://europa.eu/eurobarometer/surveys/detail/3174, 01.10.2025.

Weakening consent requirements for device access disproportionately favours data-rich, vertically integrated **platforms** due to scale and network effects, raising barriers for privacy-friendly SMEs that invested in compliant, contextual or first-party models. This undermines a level playing field and risks entrenching market power. It also runs counter to the objectives of the Digital Markets Act (DMA), which seeks to limit gatekeeper leverage and promote fair competition in the digital economy. Privacy-enhancing innovation flourishes when the rules are clear and enforced. vzbv therefore favours structural risk reductions, shifting investment towards contextual, first-party and non-individualised approaches.

Lowering consent prompts without **closing the enforcement gap** yields only cosmetic gains. Effective reform must combine ePrivacy safeguards with resourced data protection authorities (DPAs) and coordinated cross-border action; registries and certification for ad-ecosystem actors; and alignment with DSA ad-transparency repositories and DMA consent constraints.

> Any ePrivacy reform should streamline the user experience without diluting the Charter-level protections in the ePrivacy Directive and the GDPR. **The way forward is to reduce structural risks by prohibiting tracking and profiling for advertising and to strengthen coordinated enforcement**,[7] **and not expanding consent-free access to terminal equipment.** This approach reduces consent noise while strengthening user control and fair competition. Strong rules affirm the EU's role as a global leader and reinforce digital sovereignty. They keep rights at the core of Europe's digital future and uphold the European Commission's commitment to protect its citizens.

The European Commission's intentions to reduce the number of consent prompts can be beneficial - if and only if systemic tracking practices decline, meaning that advertising practices are reduced to privacy preserving approaches rather than shifted into consent-free carve-outs. However, if the reform shifts more processing into consent-free categories (e.g. by introducing "legitimate interest" as a legal basis, broadening "strictly necessary" or introducing compatibility presumptions for ad-funded media), it lowers transparency, expands dark-pattern leeway and erodes users' effective choice. This contradicts established case law and invites legal uncertainty.

Centralised preference tools are only effective if legally binding, machine-readable signals are recognised, identifiers are not repurposed into cross-service tracking (e.g. advertising IDs, device IDs, login-based IDs) and governance prevents gatekeeper leverage at browser or operating system level. Voluntary tools without binding effect often serve AdTech interests rather than users.

If the European Commission aligns ePrivacy rules more closely with the GDPR, it must be borne in mind that privacy and confidentiality of communications under Articles 7 and 8 of the Charter of Fundamental Rights protect not only the processing of personal data but any access by third parties to users' devices. This is especially relevant when access is used for tracking and profiling for advertising.

---

[7] These positions and demands are set out in detail in Verbraucherzentrale Bundesverband (vzbv) (2025) (wie Anm. 1).

> Overall, the adjustments outlined by the European Commission carry a serious risk of undermining the protection of fundamental rights and should be accompanied by an independent assessment of impacts on fundamental rights.

2. General Data Protection Regulation

Although the European Commission's Call for Evidence does not suggest any adjustment of the General Data Protection Regulation (GDPR), there are numerous political voices calling for the deregulation of data protection. Against this backdrop, it should be recalled that **the GDPR is a European success story and constitutes a central pillar of its digital regulatory framework**. It is the outcome of an intensive multi-year negotiation process in which legislators, civil society, business and academia were equally involved. As such, the GDPR represents a carefully balanced compromise reconciling different, partly conflicting interests. It subsequently served as a reference model for data protection laws in numerous third countries.

From the perspective of vzbv, it would be **misguided to portray data protection as a general obstacle to competitiveness** and technological innovation. There is no robust empirical evidence demonstrating that strong data protection hinders innovation.[8] On the contrary, the European Commission's evaluation reports from 2020 and 2024 as well as stakeholder feedback confirm that there **is no structural need for reform of the GDPR**. The Commission itself stressed that the principles and rules of the GDPR are effective, future-proof and proportionate.[9] Likewise, during the GDPR Implementation Dialog[10] led by Commissioner for Democracy, Justice, Rule of Law and Consumer Protection Michael McGrath in July 2025 it became clear that stakeholders overall perceive the GDPR as a balanced legal framework that has achieved its objectives. European business associations emphasised that they have invested heavily in GDPR compliance and that a fundamental reopening of the legal framework would create new uncertainties.

The Council of the European Union reached a similar conclusion: in its 2023 report[11] it described the GDPR as a success. It has delivered positive results in harmonising EU law and strengthening a culture of data protection at EU and global level. Its application has increased trust and legal certainty, facilitated cross-border data flows within the EU and thereby supported the single market as well as the development of the digital economy. The focus should therefore remain on coherent interpretation and effective enforcement rather than deregulation.

It is not data protection or consumer protection that hampers Europe's competitiveness and capacity for innovation but structural deficits: insufficient digitalisation of public administration, slow expansion of digital infrastructures (like fibre and 5G networks), persistent shortages of skilled workers and a lack of investment in research, development and start-up support. Strong data protection, by contrast, is a cornerstone of a value-based digital economy and a European promise

---

[8] See Bernd Beckert u. a.: Die Digitalisierung aus Innovationsperspektive. Faktencheck und Handlungsbedarf. Policy Brief 01/2021, S. 13, https://www.isi.fraunhofer.de/content/dam/isi/dokumente/policy-briefs/policy_brief_digitalisierung.pdf, 02.10.2025.

[9] European Commission: Second Report on the application of the General Data Protection Regulation. COM(2024) 357 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0357, 02.10.2025.

[10] Dass.: GDPR Implementation Dialogue: Summary Conclusions, 2025, https://commission.europa.eu/document/download/835dfd02-a38c-4cc3-ba53-5b0499e2b8b9_en?filename=Summary%20Conclusions%20Implementation%20Dialogue%20on%20the%20GDPR.pdf, 02.10.2025.

[11] Council of the European Union: Council position and findings on the application of the General Data Protection Regulation (GDPR). 15507/23, https://data.consilium.europa.eu/doc/document/ST-15507-2023-INIT/en/pdf, 02.10.2025.

of quality. Numerous European companies – for example in the field of privacy-friendly AI applications – are successfully positioned on the market on this basis.[12] By contrast, a lower level of protection would primarily benefit data-rich, market-dominant corporations at the expense of medium-sized enterprises.

For consumers, data protection means simplification and reduction of bureaucracy in everyday life as they can rely on a high level of protection when using digital services. At the same time, consumer trust is an essential prerequisite for the uptake of digital services and for strong brand loyalty. Studies, however, show that data protection concerns are among the main reasons why consumers avoid certain digital services.[13]

It must also be considered that **any proposed adjustments could lead to further erosion** of the GDPR. In the political debate – for example from the German Federal Government – proposals have been put forward to exempt SMEs entirely from the scope of the GDPR.[14] The Danish Council Presidency has already suggested restricting the rights to information and access under Articles 13 to 15 GDPR and making the right to lodge a complaint under Article 77 more difficult. [15] These initiatives show that even the smallest adjustment could serve as a gateway to massively undermining the carefully balanced regulatory framework of the GDPR, with the result of a profound erosion of the European level of protection.

Furthermore, the GDPR together with the Digital Services Act (DSA), the Digital Markets Act (DMA) and other instruments form the **foundation of a coherent European regulatory framework** for the digital sphere. This framework provides predictability and thereby legal, planning and investment certainty for companies. There is a risk that reform would undermine the coherence of this regulatory framework – which has not yet been fully implemented – and run counter to the stated objectives of simplification and predictability of EU law. In particular, it would weaken the principle of a graduated yet uniform level of protection for fundamental rights in the digital space.

Only if the existing instruments are strong, consistent and strictly enforced can **the European Union maintain its role as a global standard-setter** in the field of digital fundamental rights. They strengthen Europe's independence from non-European platforms – particularly in view of growing geopolitical tensions and international competitive dynamics. Any reopening risks gradually eroding the level of protection – with far-reaching consequences for fundamental rights, legal certainty and trust.

> The GDPR is a proven legal framework for the digital space and does not require structural reform. The European Commission should focus on coherent interpretation and consistent enforcement. Therefore, the European legislator should invest in awareness-raising, technical support and consistent enforcement to strengthen a digital regulatory framework that guarantees competitiveness, innovation and fundamental rights protection alike.

---

[12] Including for example Brighter AI and Sordi.ai, among others.

[13] Bitkom: Mehr als jeder Dritte hat Hemmungen, digitale Angebote zu nutzen, 2025, https://www.bitkom.org/Presse/Presseinformation/Hemmungen-digitale-Angebote-Digitaltag-2025, 02.10.2025.

[14] Bundesregierung: Koalitionsvertrag zwischen CDU, CSU und SPD. 21. Legislaturperiode, 2025, S. 65, https://www.cdu.de/app/uploads/2025/04/Koalitionsvertrag-%E2%80%93-barrierefreie-Version.pdf, 02.10.2025.

[15] Danish presidency of the Council of the European Union: Securing better conditions for companies to comply with the data protection rules. DK Non-paper, 2025.

This includes, for example:[16]

- The European Commission, together with the European supervisory authorities, should work to develop and actively disseminate easy-to-understand, harmonised guidance, templates and checklists specifically for SMEs.
- The European Commission should work to ensure that the risk-based approach of the GDPR is genuinely implemented and that companies can benefit from simplified documentation requirements when processing data with low risk.
- The European Commission should provide standardised, approved contractual clauses and model texts (e.g. for data processing agreements) that companies can directly use to achieve legal certainty and reduce compliance costs.
- The European Commission should develop and release uniform short texts and pictograms for typical processing operations so that SMEs can fulfil their information obligations more efficiently while also strengthening transparency for consumers.
- The European Commission should actively promote the development of sector-specific codes of conduct and SME-appropriate certification schemes and advocate for pragmatic recognition practices.
- The European Commission should ensure that Member States equip their data protection supervisory authorities with sufficient staff and financial resources to expand their support for SMEs.

3. Artificial Intelligence Act

Simplifying and aligning the Artificial Intelligence Act (AI Act) with other legal frameworks, such as the General Data Protection Regulation (GDPR), can enhance legal certainty and enforcement. However, vzbv strongly cautions against any form of deregulation or weakening of key safeguards in the AI Act under the guise of simplification. The AI Act is a landmark instrument for protecting consumers and fundamental rights in an economy increasingly driven by AI-systems. The AI Acts core provisions on prohibitions, high risk AI systems and GPAI protect consumers directly and indirectly must not be diluted. This holds in particularly for the provisions in the Chapters 2, 3, 4 and 5.

> Weakening the provisions in the AI Act - such as by narrowing scope of high-risk AI or hollowing out providers and deployers obligations - significantly undermines consumer protection. When the Digital Omnibus aims to consolidate and standardise these provisions and reporting and documentation obligations with those in other legal acts it must not lead to a weakening of these obligations and safeguards that ensure consumer protection.

This includes:

[16] These positions and demands are set out in detail in Verbraucherzentrale Bundesverband (vzbv) (2025) (wie Anm. 2).

- No delay in the application of the AI Act – the Commission must not introduce a “Stop-the-Clock” mechanism that postpones the enforcement of key consumer rights and obligations for providers and deployers, such as labelling obligations for high-risk AI.
- No exemptions or weaker rules for SMEs and mid-caps – obligations must be based on risk of AI systems, not company size.
- No narrowing of the scope of high-risk AI: No exclusion of Annex I, no limitation of scope of Annex III or weakening the high-risk AI classification mechanism in Art. 6.
- No weakening of provisions on prohibited AI-practices in Art. 5.
- No weakening of the core provisions on high-risk AI and GPAI as they ensure proper risk management, risk mitigation, data quality, fairness, accuracy, robustness of outcomes and transparency.
- No weakening of labelling and transparency obligations for high-risk AI systems (Art. 26 (11)) and certain AI systems (Art. 50).
- No weakening of the right to explanation of high-risk AI-decisions in the AI Act (Art 86) and the the GDPR (Art. 22).

Explanations and background information on the individual demands are listed below:

No “Stop-the-Clock”: vzbv firmly opposes any “Stop-the-Clock” mechanism that would delay the application of the AI Act. Such a delay allows AI-related risks to persist while denying consumers the few enforceable rights they have under the AI-Act such as the right to an explanation of high-risk AI decisions.

Postponing the classification of high-risk AI and the obligation for labelling obligations for high-risk AI systems (Art. 26, (11)) would make it impossible for consumers to recognise high-risk-AI and demand an explanation on individual decisions according to Art. 86. Also, consumer organisations could not monitor and enforce compliance, including the prohibitions under Art. 5 when AI systems – especially high-risk AI systems - are not labelled as such.

Moreover, a delay would send a damaging political signal. If the Commission yields to pressure from a narrow group of industry actors and sacrifices consumer rights for short-term commercial interests, public trust in the EU’s commitment to protecting people over corporate players will erode. This risk is undermining the legitimacy of digital regulation and weakening democratic confidence in European institutions.

> No delay of application of AI-Act provision - No “Stop-the-Clock” mechanism, as it exposes consumers to various high-risk AI without any safeguards, make it impossible for consumers to demand an explanation on individual high-risk-AI decisions according to Art. 86 and impedes consumer organisations enforcing of the prohibitions under Art. 5.

No exemptions or weaker rules for SMEs and mid-caps: Even AI systems developed or operated by small companies can have significant adverse impacts on individuals. Therefore, there must be no weaker rules or additional exemptions for SMEs or mid-cap companies under the Digital Omnibus.

> No exemptions or weaker rules for SMEs and mid-caps as the AI Act's obligations are risk-based and proportionate to the potential harm posed by an AI system. The size of the company providing or deploying such a system is irrelevant to the risk it poses to consumers.

No narrowing of the scope of high-risk AI: Narrowing the scope of high-risk AI systems would dismantle key safeguards for consumers as consumers would be exposed to high-risk AI systems without the safeguards the AI Act provides. AI systems covered in the sections of Annex III on biometrics, education or credit scoring and insurance affect consumers must remain subject to strict requirements. The AI Acts provisions on high-risk AI systems are complementary to existing sector regulation. Therefore, the Digital Omnibus must not exclude Annex I from the AI Act, as this would expose consumers to AI-related risks that are not sufficiently addressed in the corresponding sector regulation.

> No narrowing of the scope of high-risk AI: No exclusion of Annex I, no limitation of scope of Annex III or weakening the high-risk AI classification mechanism in Art. 6.

No weakening of the core provisions on high-risk AI and GPAI: The AI Act aims to promote human-centric and trustworthy AI in Europe. Core provision of providers and deployers of High-Risk-AI constitute essential safeguards for consumers, including:

- Risk management and mitigation duties for high-risk AI systems (Art. 9 ff.).
- Requirements for data quality and representativeness (Art. 10).
- Accuracy, robustness, and cybersecurity for high-risk AI systems (Art. 15).
- Obligations for providers for general-purpose AI models (GPAI) (Art. 53 AI Act) and obligations for providers of GPAI with systemic risk (Art. 55).

These core provisions and obligations for providers and deployers aim at securing the systems run non-discriminatory and provide an accurate output. Thereby the provisions protect consumers directly and indirectly must not be diluted. This holds in particularly for the provisions in the Chapters 2, 3, 4 and 5.

> No weakening of the core provisions on high-risk AI and GPAI as they ensure proper risk management, risk mitigation, data quality, fairness, accuracy, robustness of outcomes and transparency.

No weakening of provisions on prohibited AI-practices: Art. 5 already contains wide loopholes that allow the manipulation and exploitation of large groups of consumers through AI systems. The prohibitions in Art 5 are already weak and must not be watered down further.

> No weakening of provisions on prohibited AI-practices in Art. 5 including manipulative practices, exploitation of vulnerabilities, unfair use and discriminatory use of AI.

No weakening of labelling and transparency obligations: Clear labelling and transparency are essential for consumer autonomy. Labelling and transparency obligations for providers and deployers of certain AI systems (Art. 50) as well as high-risk AI systems (Art. 26 (11)) must not be weakened. They are the precondition for consumers to exercise demand an explanation on individual decisions according to Art. 86. Consumer organisations cannot monitor and enforce compliance, including the prohibitions under Art. 5 when AI systems are not labelled as such.

> No weakening of labelling and transparency obligations for high-risk AI systems (Art. 26 (11)) and certain AI systems (Art. 50) as it would undermine consumer autonomy and enforcement of the AI Act.

No weakening of the right to explanation of high-risk AI-decisions in the AI Act and the right to explanation of automated decisions in the GDPR: Art. 22 GDPR grants consumers the right to an explanation only in cases of fully automated decisions with legal or similarly significant effects. Art. 86 of the AI Act goes further by granting a right to an explanation of individual decisions based on high-risk AI systems, even if a human is involved, but is restricted to high-risk-AI systems. So, both provisions are complementary. Harmonisation of both must not reduce the scope of either right. Consumers must receive meaningful explanations in all relevant scenarios—regardless of whether it is about an automated decision according to the GDPR or for a high-risk AI- based decision where a human may be involved under the AI Act.

> Clarification yes, but no weakening of the right to explanation of high-risk AI-decisions (Art. 86) in the AI Act and the right to explanation of automated decisions in the GDPR (Art.22).

4. Cybersecurity related incident reporting obligations

vzbv welcomed the provision in the Cyber Resilience Act (CRA) requiring manufacturers to inform users about actively exploited vulnerabilities and significant cybersecurity incidents and strongly supported the obligation for market surveillance authorities to establish accessible complaint and reporting mechanisms, enabling consumers to report security breaches or potential violations of the legislation. These measures represented a meaningful step toward greater transparency, accountability, and consumer empowerment in the digital product landscape.

When manufacturers are obliged to inform users about actively exploited vulnerabilities and serious security incidents, consumers can make informed decisions, take protective actions, and avoid potential harm. Additionally, accessible complaint and reporting mechanisms empower consumers to directly alert authorities about unsafe products or legal violations, helping to ensure faster enforcement and better protection. These measures foster trust, improve safety, and give consumers a stronger voice in the digital ecosystem.

Simplified and harmonized reporting obligations under the Digital Omnibus can enhance transparency and efficiency by ensuring that cybersecurity incidents are communicated clearly and consistently across the EU. However, there is a risk that simplification may reduce the depth or frequency of reporting, potentially delaying critical information or limiting consumers' ability to act.

Therefore, simplification must be carefully balanced to maintain robust consumer protections while improving clarity and responsiveness.

> Simplification should aim to **streamline procedures**, not reduce the quality or frequency of reporting. A well-designed system will empower consumers, support enforcement, and strengthen trust in the digital product market.

5. Responsibility of operators of online marketplaces

Unnecessary bureaucracy is a burden for business and consumers, but reporting obligations are not the reason why European business is complaining about profit declines. The reason why business is heavenly under pressure is unfair competition. Nowhere is this more apparent than in e-commerce. Everyday millions of small parcels with non-compliant products enter the border of the European Union – damaging European business and consumers.

With the Digital Services Act (DSA) and the General Product Safety Regulation (GPSR) due diligence obligations for operators of online marketplaces were introduced. But the legal obligations are not in line with the significant influence operators of online marketplaces have. Without their services, purchasing contracts would not be concluded in such high numbers. New operators in the market both reinforce existing problems and add new ones.

A sweep lately published by the European Commission shows: There are still far too many offers online that do not meet the formal requirements.[17] These findings are consistent with vzbv research.[18] The results show that enforcement is key. But it is also key to close regulatory gaps were evident. The major weakness in enforcing EU law against third-country companies and ensuring a level playing field is the abstinence of a responsible economic operator. In order to achieve a possibly strong, noticeable and lasting effect it is important to go to the very root of the problem. The European Commission has to give responsibility and accountability to those making the money.

> Operators of online marketplaces should take more responsibility when third-party traders infringe EU law. Additional targeted due diligence obligations should be introduced. Responsibility must be supported with accountability: Operators of online marketplaces should be subject to joint and several liability alongside traders for infringements. [19]

[17] European Commission: First sweep under new product safety rules shows that while basic requirements are broadly met, more needs to be done to ensure that consumers and relevant authorities get all relevant safety information, https://ec.europa.eu/commission/presscorner/detail/en/mex_25_1879, 06.10.2025.

[18] vzbv: Online-Shopping: Wichtige Produktinformationen fehlen häufig, https://www.vzbv.de/pressemitteilungen/online-shopping-wichtige-produktinformationen-fehlen-haeufig, 06.10.2025.

[19] These positions and demands are set out in detail in Verbraucherzentrale Bundesverband (vzbv) (2025) (wie Anm. 1).

Imprint

Published by:
Federation of German Consumer Organisations
Verbraucherzentrale Bundesverband e.V.
Rudi-Dutschke-Straße 17, 10969 Berlin

Team Digital and Media
digitales@vzbv.de
vzbv.de