

Digital Omnibus: Digital Package for Simplification

Video Games Europe's contribution to the European Commission Call for Evidence

Video Games Europe welcomes measures aimed at reducing regulatory fragmentation and promoting simplification. Our members make significant investments in creating and producing content, and are faced with increasing digital regulation, potentially leading to competitive disadvantages on a global level. The last decade has seen the introduction of GDPR, DSA, DMA, DCD, the New Deal Omnibus, the Data Act, the Data Governance Act, the AI Act and more. Businesses face overlapping demands across consumer protection, data protection, communications law, and more. This Commission is also proposing to add to those overlapping rules with a Digital Fairness Act.

We agree that now is the time to consider how to streamline and rationalise the demands on businesses to ensure that European citizens can be protected, while the European economy remains competitive. Video Games Europe is keen to work with the Commission on potential areas for simplification, including in these laws. It is crucial that any measures aiming at simplification de facto reduce regulatory and administrative burdens for companies. Therefore, we caution against such measures when they bring new convoluted compliance challenges. In this paper, we will reflect on our observations in relation to the main stated objectives in the Call for Evidence document associated with this consultation.

Executive summary

- For data transfers outside the EU, full legal certainty is required, in particular where these depend on standard contractual clauses
- For the roll-out of the Data Act, a grace period is needed to ensure a better and safer user experience
- For the application of the GDPR, adjustments are needed to restore consistency and to reduce burden on companies
- For ePrivacy, data processing for online safety reasons needs to continue
- For the Cyber Resilience Act, further guidance is needed, namely on scope and on what constitutes a 'substantial modification'
- For the implementation of the AI Act, a proportionate application is needed, taking into account the low risk of video games

Data transfers outside the EU: full legal certainty needed

1. Video Games Europe had the opportunity to respond to the Call for Evidence on the Data Union Strategy. Data is not just fundamental for the development and creation of new video game content; it also plays an essential role in ensuring that consumers can access and purchase this content and that they can enjoy a good and frictionless gameplay experience.
2. The video games industry today is a global business, and video game companies offer their services/products to video game players across the world. Our members are only able to deliver their services/products to their customers if they are in a position to process user data across borders. The industry, therefore, depends on international data flows and a harmonised legal framework that provides uniform rules across territories, in particular in relation to the transfer of personal data outside the EU. While the European Commission is making important efforts to create new adequacy agreements under the GDPR, such as the EU-U.S. Data Privacy Framework, data transfers often still take place under a legal framework based on Standard Contractual Clauses (SCCs) that require additional safeguards, transfer impact assessments, provision of information, etc.
3. We call on European policymakers to consider ways of increasing legal certainty in relation to these types of data transfers. This could be done by developing additional guidance on how SCCs should be used in a broader commercial context, such as clarifying the consequences of termination of SCCs for the underlying commercial contract, explaining the interaction of SCCs with processing operations that are conducted under the GDPR, or providing specific guidance on how to conduct transfer impact assessments. Furthermore, it should be confirmed that SCCs can be incorporated by reference in an underlying agreement without a separate signature if both parties accept the terms of the underlying agreement.

Data Act: roll-out challenges and potential grace period

4. Data access and sharing can generate a wide range of benefits, including facilitating collaboration and the harnessing of new and existing data sources to foster data-driven innovation. The Data Union Strategy should contribute to facilitating such cross-border data sharing and leverage its collaborative benefits, which will foster the free flow of qualitative data and help establish the “Single Market for Data”. European video game companies are reliant on data flows to scale and grow. It is therefore essential that European policy makers continue their work on mechanisms supporting international data flows, and oppose data localisation policies which undermine the principle of free flow of data across borders, as these create barriers to the smooth functioning of the market. [A recent OECD study](#) quantified the economic impact of structural data localisation and restriction of data flows. According to this study, data autarky - or full fragmentation, where all economies fully

restrict their data flows - would result in global GDP losses of 4.5% and reductions in exports of 8.5%.

5. The Data Act is one of the cornerstones of the “Single Market for Data”. However, it adopted a limited timeframe during which manufacturers need to adapt their products, allowing easy access by design to various types of data. This limited time frame is problematic for products with long development cycles, such as video game consoles. Implementation of the Act has led to uncertainty about how to interpret the new rules, in particular in relation to (i) the differentiation between types of data, (ii) the identification and consideration for protection of business and trade secrets and (iii) the practical unclarities regarding its overlap with GDPR.
6. As part of its efforts to reduce the burden on companies, Video Games Europe calls on the Commission to consider granting additional lead-time to companies. Such a prolongation would need to come fast. This will allow companies to prepare the internal processes and roll out updates to their devices, which, in turn, will ensure better protection against data leaks and/or hacking, thereby guaranteeing a safer user experience.

GDPR: consistent application and burden adjustments

7. The GDPR has been successful in achieving its objectives in guaranteeing the protection of individuals' data in an effective and comprehensive manner while enabling data-driven growth. Its principles and its risk-based approach continue to provide a strong foundation for personal data governance and for the protection of Europeans' fundamental rights more broadly, which underpins the broader digital regulatory framework. However, since its entry into application, various interpretation and enforcement issues have emerged, leading to a lack of consistent application, legal uncertainty and unnecessary barriers to innovation, as reported in the Commission's Second Report on the application of the GDPR. In addition, several national exemptions in the law allow flexibility for Member States, for instance, in determining the age of children's consent in relation to information society services, which also created diverging national practices. While Video Games Europe does not support a full reopening of the GDPR, minimal adjustments in the context of the upcoming Digital Omnibus could bring some relief and clarity. For example, such adjustments could be to impose statutory duties for all digital regulators to find compromise solutions where there is overlap with other digital laws, and/or duties for data protection authorities (DPAs) to strive towards a harmonised decision praxis in the EU.
8. Video Games Europe welcomes the [Helsinki statement](#) on enhanced clarity, support and engagement adopted by the European Data Protection Board (EDPB), outlining its plan to support simplification of GDPR compliance. The EDPB's commitment to strengthen its dialogue with stakeholders, provide new tools to make GDPR

application easier, enhance consistency of application and enforcement by DPAs and proactively engage with other regulators will certainly help address the lack of consistency in applying the GDPR and foster a culture of trusted innovation. We call on the DPAs to adopt similar commitments and would welcome it if they could be formalised as part of the Commission's forthcoming work on the omnibus packages.

9. We caution against the challenges that companies face when data subject rights are misused for improper purposes to burden data controllers. This happens, for instance, when users abuse their right to access and demand data simply to tie up company resources as retribution for some non-data-related grievance they may have, or when they do so to gain an undue advantage in civil disputes unrelated to data processing. Another example of this is when users who have licensed Intellectual Property Rights to a company raise access requests and threaten objections to the processing of their data unless the company pays them a further licence fee. We believe that this can be addressed via adjustments to the legal framework, allowing controllers to filter and/or refuse requests that, because of their context and/or scope, are seemingly (or clearly) not aimed at the purpose foreseen by law.

ePrivacy: data processing for online safety reasons needs to continue

10. Video Games Europe recommends rethinking this instrument holistically rather than just updating the existing provisions. Particularly, it should be assessed carefully which provisions in the ePrivacy Directive (ePD) are outdated or have been superseded by legislative or technological developments.
11. While the confidentiality rules should be modernised and adapted to the current environment, allowing for automated processing of communications for goals that benefit users, for video game companies, it is of utmost importance not to be restricted in their ability to protect users, especially children, from harassment, bullying, grooming, hate speech and cheating. Therefore, in the context of a simplification exercise, the processing of communications data according to the ePD must continue to be allowed to ensure not just the security of the service, but also the safety of its users. We understand that there may be other provisions in the ePD that may be beneficial to address in other instruments for further simplification, but we respectfully ask to maintain the current framework that allows video game companies to keep in-game communications safe.
12. The rules on the processing of traffic and location data in (Articles 5-6 and 9 ePD), on direct marketing (Article 13 ePD), and on storing of information or gaining access to information already stored in a user's terminal equipment ("cookie rules" - Article 5(3) ePD) could be absorbed by the GDPR. The cookie rule could, however, also be rendered more flexible by allowing cookie placement without consent in a wider range of circumstances, e.g. for security, software updates, anti-fraud, and analytics. For

instance, one proposal that we would support is to exempt the collection and processing of end-users' data for technical purposes and for conducting simple statistics on the functioning and use of websites from prior consent in order to help companies reduce costs related to implementing and maintaining cookie banners. An example of such an exemption may be found in the 2025 UK Data (Use and Access) Act. A similar provision on the EU level would ensure consistency for businesses operating cross-border website services.

13. These changes would make the future ePrivacy framework leaner and clearer, which would reduce the currently existing overlaps between data and privacy laws and harmonise their application, improve legal certainty, and allow for enhanced yet rules-based innovation of communication services offered in the EU.

Cybersecurity: further clarity and guidance needed

14. The video game industry is one of the fastest-growing digital sectors in Europe, with millions of users engaging through online platforms, multiplayer services, and digital marketplaces. This makes it a key testbed for robust cybersecurity standards. Video game platforms that include online interaction and purchase functions are sometimes targets of cyberattacks, ranging from account takeovers and data breaches to distributed denial-of-service (DDoS) attacks.
15. Some major video game ecosystems rely on extensive third-party integrations such as mods, digital distribution services, and user-generated content platforms. The Omnibus should therefore encourage voluntary secure software development practices. This would not only mitigate risks but also create trust in a sector where reputation and player safety are vital for sustainable growth. In this vein, we would like to take the opportunity to highlight that the scope of the Cyber Resilience Act (CRA) is not clearly defined, as is the issue of the notion of 'substantial modification', and recall that the Commission is empowered to provide guidance under Article 26(2)a) and d) of the CRA.
16. Further guidance is also needed for another point in CRA: it is not clear how to put the 'CE' marking on software products in case such software is distributed on dedicated app stores. Additionally, a security update period for 10 years after release of the update (Article 13(9) CRA) is too long for products like video game consoles.
17. As stated in Article 30 CRA, "*for products with digital elements which are in the form of software, the CE marking shall be affixed either to the EU declaration of conformity referred to in Article 28 or on the website accompanying the software product*". Video Games Europe asks the Commission to provide clarity on what is understood by 'the website accompanying the product'.

18. In addition, there are further open questions: what would be the criteria to establish that the website does “accompany” the product? Should that webpage be clearly referenced in the software as a redirection point for more information/customer support, or would any page broadly presenting the product and its characteristics be understood as a webpage accompanying the product? If the latter, does this mean that any page broadly presenting the product should have a CE marking? All these questions should be answered by future guidance, and Video Games Europe stands ready to support in the creation of such guidance.
19. Finally, because video game communities span across borders, cybersecurity challenges in this industry are inherently transnational. Video Games Europe’s members are committed to promoting a culture of security by design in video games, where security and privacy are embedded from the outset of game and platform development, to enhance consumer trust, reduce systemic risks, and strengthen Europe’s leadership in the global digital entertainment economy.

Contact

- Ann Becker - SVP, Head of Policy and Public Affairs
ann.becker@videogameseurope.eu

About Video Games Europe

Since 1998, Video Games Europe has ensured that the voice of a responsible video games ecosystem is heard and understood. Its mission is to support and celebrate the sector’s creative and economic potential and to ensure that players around the world enjoy the benefits of great video game playing experiences. Europe’s video games sector is worth €26.8bn and accounts for 116.000 jobs. 54% of Europeans are video game players. We publish a yearly [Key Facts](#) report with the latest data on Europe’s video games sector.

www.videogameseurope.eu