INTERACTIVE SOFTWARE
FEDERATION OF EUROPE
Representing the European video games industry

Trialogue negotiations on the proposal for an e-Privacy Regulation
Key considerations from the video games industry

The Interactive Software Federation of Europe (ISFE) represents the European video games industry. ISFE's membership comprises 17 major publishers and national trade associations in 15 countries throughout Europe. Our national associations in turn represent hundreds of games companies across Europe that produce and publish interactive entertainment and educational software for use on personal computers, game consoles, portable devices, mobile phones and the Internet.

The video games sector represents one of Europe's most compelling economic success stories. In terms of consumer spend, the European video games market was worth an estimated €23bn in 2020, and registered a growth rate of 22% over the previous year. The industry now includes some 5,100 European game developer studios and publishers that enjoy an estimated combined annual turnover of €12bn and that employ approximately 90,000 people across the continent[1].

ISFE members call on all trialogue negotiators to aim for an agreement that ensures GDPR consistency and legal certainty for users and businesses and finds the right balance between the high-level protection of the fundamental rights to private life and protection of personal data on electronic communications on the one hand, and the ability to develop new innovative technologies and foster growth in the digital society on the other. This balance can only be achieved in the context of our sector, if following key considerations are taken into account:

Recital 11aa of the Council text which clarifies the scope of the law proposal in relation to a chat room in an online game must be maintained.

- Video games companies provide notice to players that some in-game communications may be monitored to address cheating, hate speech, bullying, grooming and harassment. A multi-faceted approach, including proactive tools that detect harmful content, and reactive reporting tools that allow players to notify it, is used to ensure the safety of the players. Active and/or reactive monitoring of chat has always played a key role in the fight against hate speech and child sexual abuse, both of which are important policy objectives.
- If all in-game communications fall within the definition of an interpersonal communication service, such monitoring would be made impossible as the ePrivacy Regulation does not allow processing of content data without consent. Securing consent in these circumstances would not work, as bad actors would have no reason to consent. Furthermore, in case of underage users, obtaining parental consent would be onerous and any delays in obtaining it could potentially jeopardize the investigation.
- ISFE members strongly welcome the clarification in Recital 11aa of the Council text that "communications in an electronic communications channel in online games which is open to all persons playing the game" do not constitute an interpersonal communication feature. It is helpful to clarify that there are forms of in-game communication that do not enable direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s).

[1] ISFE EGDF Key Facts 2020 from GameTrack Data by Ipsos MORI.

- However, **the ePrivacy Regulation should not restrict video game companies' ability to protect users, especially children, from harassment, bullying, grooming, hate speech and cheating.** Where ancillary communications fall within the scope of an interpersonal communication service, the processing of communications data should be allowed to ensure not just the security of the service (Art. 6.1.b), but also the safety of its users. We call on the negotiators to allow companies to filter out potentially harmful content in communications services that are addressed to children in order to ensure a safe and inclusive environment.

Article 8 (*Protection of end-users' terminal equipment information)*: The Council versions of Articles 8.1(c), 8.1(d), 8.1(da) and 8.1(e) should be adopted in their broadest possible form.

- Gameplay services may have to rely on the processing and storage capabilities of a user's device to ensure that the game performs properly and remains challenging and compelling. Service providers may, for instance, need to collect information about potential bottlenecks within the game or measure the performance of the service.
- Service providers should not have to rely on individual requests for specific consent in such situations that do not raise any genuine privacy concerns. This will lead to consent fatigue or in case of underaged users, a cumbersome parental consent process.
- The Council versions of the provisions allowing to rely without consent on the processing and storage capabilities of the user's device for the technical delivery of the service (8.1(c)), for audience measuring (8.1(d)), "for the purpose of maintaining or restoring the security of information society services, preventing fraud or detecting technical faults" and regarding software updates (8.1(e)) should therefore be adopted in their broadest possible form. In addition, third-party providers and joint controllers should be allowed to carry out audience measurements in compliance with GDPR rules, as it is provided in 8.1(d) of the Council text.

Article 10 *(Information and options for privacy settings to be provided):* ISFE supports the removal of Article 10.

- Imposing privacy settings on operating software would remove any incentive for third party providers to innovate and offer better privacy-friendly services than their competitors which may result in less rather than more protection of users' privacy. It would also concentrate power in the hands of a few software companies and deprive consumers of the ability to share more data with the companies that they trust.
- It would also be extremely cumbersome and costly to impose such settings on browsers provided as an ancillary service on a games console which is no longer commercially distributed.

Article 11 *(Restrictions)* should be aligned with Article 23 of the GDPR and include additional references to Articles 23.1(i) and (j) as the Council text provides.

- Article 11 should not prevent national law enforcement to have the necessary means to investigate IP infringements and right holders to effectively pursue civil law claims. To effectively implement Article 8 IPRED, Member States must be allowed to impose limited exemptions from confidentiality of communications for the protection of the fundamental rights and freedoms of others and for the enforcement of civil law claims.
- The list of general public interests that would allow such an exemption in Article 11.1 should therefore be expanded with a reference to Articles 23.1 (i)"the protection of the data subject or the rights and freedoms of others" and 23.1(j)"the enforcement of civil law claims" in the GDPR.

ISFE Secretariat, November 2021