Public Consultation on the EDPB's Guidelines 01/2024 on the Processing of Personal Data based on Article 6(1)(f) GDPR

Response from VIDEO GAMES EUROPE

Transparency Register Identification Number: 20586492362-11

1. Video Games Europe welcomes the opportunity to provide comments on the draft Guidelines 01/2024 on the Processing of Personal Data based on Article 6(1)(f) GDPR by the European Data Protection Board (EDPB). Our members welcome the issuing of Guidelines and Recommendations by the EDPB as they promote a common understanding of the European data protection framework and provide a harmonised interpretation of key provisions in the GDPR. This will help to ensure an effective and meaningful implementation of the GPDR.

2. These Guidelines will be of great value to our sector and will help companies to process personal data lawfully and fairly. Overall, however, we find that the guidance is very restrictive in nature and provides mainly examples where the use of the legitimate interest basis is not allowed or restricted, rather than examples of a recommended and correct use of this legal basis. Such a one-sided approach may not lead to an objective and balanced interpretation of the legal framework and will hinder, rather than support, a correct implementation of the rules. We would welcome the addition of examples of appropriate application of legitimate interests and the balancing test.

3. We have also identified a number of interpretation issues in the text that do not appear to be in line with the legal framework of the GDPR and related case law. We will highlight these in our comments below, following the order of the table of contents and corresponding paragraph numbers. The most important points that we wish to make are:
    - It should be clarified what is meant by *"the chilling effect on protected behaviour"* and how this would restrict the use of a legitimate interest basis.
    - The Guidelines should more closely align with the CJEU ruling in **Meta v. Bundeskartellamt** (Case C-252/21) and provide practical examples of relying on legitimate interests as the legal basis for product improvement in compliance with data minimisation.
    - The requirement to provide documentation on the balancing test to data subjects, and not just data protection authorities, exceeds the requirements of Articles 13 and 14 GDPR and may defeat the purpose of some processing (for example by disclosing the specific information processed to detect fraud, enabling bad actors to evade detection).
    - The right to object to the processing of personal data and the right to erasure of such data should be kept separate.

- The notion of harm should be considered a sufficiently compelling ground, and its threshold should not be raised with the notion *"immediate"*. Additionally, protecting individuals (and not just organisations) from serious harm should be considered a sufficiently compelling ground.
- Children's data merits special safeguards, but children's right to privacy is not by default greater than their other rights.
- The need to apply specific safeguards when children's data is processed does not automatically prohibit the use of the legitimate interest basis.
- Specific information about the data that is needed to prevent fraud should be considered a trade secret, the disclosure of which may defeat the purpose of the processing and enable bad actors to evade fraud detection, and should not be disclosed to the data subject.
- It should be clarified which other means of communication, in addition to email, SMS and MMS, require prior consent for the sending of unsolicited communications for purposes of direct marketing under the ePrivacy Directive.
- It should be clarified which other means would be as effective as direct marketing to pursue a marketing interest and less restrictive of the fundamental freedoms and rights of the data subjects.

ELEMENTS TO BE TAKEN INTO ACCOUNT WHEN ASSESSING THE APPLICABLITY OF ARTICLE 6(1)(F) GDPR AS A LEGAL BASIS

1st step: Pursuit of a legitimate interest by the controller or by a third party

4. In §18, the Guidelines rightly refer to recital 47 GDPR which clarifies that a "*legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller*". We would like to highlight in this context that the Court of Justice (CJEU) confirmed in the ruling **Koninklijke Nederlandse Lawn Tennisbond** (Case C-621/22) that the concept of legitimate interest should not be interpreted narrowly and that a commercial interest of the controller can constitute a legitimate interest within the meaning of Article 6(1)(f) GDPR, provided that it is not contrary to the law. This information should be displayed more prominently, rather than in footnote 28 on page 8.

3rd step: Methodology for the balancing exercise

5. The Guidelines indicate in §46 that the controller may also need to take into account "*possible broader emotional impacts resulting from a data subject losing control over, personal information, or realising that it has been misused or compromised*". The text then goes on to say that "*the chilling effect on protected behaviour, such as freedom of research or freedom of expression, that may result from continuous monitoring/tracking or from the risk of being identified, should also be given due consideration*". It should be

further clarified what is meant by "the chilling effect of protected behaviour" and how this would restrict the use of a legitimate interest basis.

6. In §54, an example is given of an online social network that is financed through online advertising to illustrate the contextual elements that should be considered in the assessment of the reasonable expectations of data subjects. The Guidelines state here that "*the users of the online social network, even if it is offered for free, cannot reasonably expect that their personal data is processed for the purposes of personalised advertising, and not even for other purposes such as product improvement*". This statement is justified with a reference to §123 of the CJEU ruling in **Meta v. Bundeskartellamt** (Case C-252/21) which states that "*it appears doubtful whether, as regards the data processing at issue in the main proceedings, the 'product improvement' objective, given the scale of that processing and its significant impact on the user, as well as the fact that the user cannot reasonably expect those data to be processed by Meta Platforms Ireland, may override the interests and fundamental rights of such a user, particularly in the case where that user is a child.*" Video Games Europe therefore calls for the better alignment of the Guidelines with §123 of the CJEU ruling which allows for the possibility of legitimate interests being the legal basis for product improvement provided organisations are compliant with the data minimisation principle and the processing does not have a significant impact on the user.

RELATIONSHIP BETWEEN ARTICLE 6(1)(F) GDPR AND DATA SUBJECT RIGHTS

Transparency and information to be provided to data subjects

7. The Guidelines provide that data subjects should be specifically informed that the processing is based on Article 6(1)(f) GDPR, and that the specific legitimate interest(s) pursued must be precisely identified and communicated to the data subject in accordance with Article 13(1)(d) and 14(2)(b) GDPR. Furthermore, it is stated in §68 that *"in any case, information to the data subjects should make it clear that they can obtain information on the balancing test upon request".* The requirement to provide documentation on the balancing test to data subjects however exceeds GDPR requirements as under GDPR, organisations only need to provide the balancing test to Data Protection Authorities on request, and organisations will have to provide significantly more information than specified in Articles 13 and 14 GDPR.

8. This requirement is also likely to impose a significant administrative burden on organisations, who may have to prepare internal and external legitimate interests assessments to ensure that confidential information and trade secrets are not shared with data subjects in a way that could negatively impact the organisation and data subjects and defeat the purposes of processing. For example, if organisations rely on legitimate interests for network security or fraud prevention purposes, sharing the balancing test with information about the tools, processes, and technical organizational measures for these purposes could result in bad actors using this information to harm the organisation and its data subjects. It could allow bad actors to circumvent the

organisation's security and fraud measures, which could result in organisations potentially in breach of other legal obligations (for example, the obligation to have appropriate technical and organizational measures under Article 32 of GDPR). For these reasons, organisations should only have to provide the balancing test to Data Protection Authorities who need to maintain confidentiality with respect to any confidential information they access in the performance of their duties (Article 54 GDPR).

Right to object

9. When processing is based on a legitimate interest basis, the data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her under Article 21(1) GDPR. In such a case, the controller shall no longer process this data unless he demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject. The Guidelines explain in §73 that the grounds invoked should be essential to the controller (or to the third party in whose legitimate interest the data are being processed) to be considered compelling. An example is given of a controller who is compelled to process the personal data in order to protect its organisation or systems from serious immediate harm or from a severe penalty which would seriously affect its business.

10. Video game companies need to deploy safety and security mechanisms that process data not just to protect video game software and licensed content from unauthorised access (hacking), but also to protect the safety of players and the confidentiality of their personal data. Hacking is often done by professional organisations that make use of unauthorised access to enrich themselves. This creates harm to the business organisation and its users alike. Such harm can be qualified as serious but is not always "immediate" as security mechanisms work in a preventative way. Video Games Europe believes that the notion of harm is sufficiently essential to the controller to be considered a compelling ground. We recommend removing 'immediate' as a qualifier of the type of harm that would constitute a compelling legitimate ground.

11. Furthermore, we recommend adding an example of a controller who is compelled to continue to process the personal data of a data subject that has objected to such processing in order to protect the interests, rights and freedoms of other data subjects.

Right to erasure

12. The Guidelines claim in §77 that "*the right to erasure is often closely linked to the right to object, in particular when the processing is based on Article 6(1)(f) GDPR",* and that, therefore, "*it might happen that the data subject's request is not completely clear*." They then recommend that, in the case of a request that the controller considers to be unclear, the controller should not only take the steps required in response to an objection as a default reaction but evaluate whether the data subject actually wishes to obtain the full deletion of its data. Video Games Europe believes that the right to object to the processing of personal data and the right to erasure of such data should not be conflated and that this recommendation should be deleted.

Right to restriction of processing

13. The Guidelines explain in §88 that the data subject has the right to obtain from the controller the restriction of processing when they have objected to a processing based on Article 6(1)(f) in accordance with Article 21(1) GDPR. This restriction applies only pending the verification of whether the legitimate grounds of the controller override the rights, interests and freedoms of the data subject. The Guidelines then state that "*once that assessment has been completed, the data should be deleted if the interests, rights and freedoms of the data subject prevail*". We suspect that this recommendation again conflates the right to erasure with the right to object, which does not include a requirement to erase any data. A controller is required to delete personal data when it no longer has a use for it (i.e. the storage limitation principle), unless there are other purposes for its use with a valid legal basis, regardless of whether the interests, rights and freedoms of the data subject prevail. We call on the EDPB to clarify its reasoning.

CONTEXTUAL APPLICATION OF ARTICLE 6(1)(F) GDPR

Processing of children's personal data

14. Video Games Europe supports the EDPB's approach that the best interests of the child must be a primary consideration when a provision is to be interpreted where children are concerned. The best interest of the child is however a dynamic concept that requires a case-by-case assessment, appropriate to the specific context. Due regard should be given to all children's rights and these rights should be equal to their right to privacy and data protection. This includes their rights to seek, receive and impart information, to have equal and effective access to the digital environment in ways that are meaningful for them such as culture, leisure and play, to meet with other children, and to have their views given due weight[1]. We recommend the Guidance clarify that all children's rights should be given equal consideration.

15. The outcome of this assessment can vary depending on children's age and development stages. Parents and caregivers have an important role to play in helping their children in the realisation of their rights, as they are best positioned to assess their evolving autonomy, capacities and understanding. It is unfortunate that this important nuance is only mentioned in footnote 114 on page 26. We recommend that the EDPB gives this important consideration a more prominent place.

16. The Guidelines emphasise in §94 the need to pay attention to recital 38 GDPR which states that children merit specific protection, in particular related to the processing of their personal data for the purposes of marketing or creating personality or user profiles. They go on to state the following: "*unless controllers can demonstrate that the activities in question which rely on the processing of children's personal data do not negatively affect the children's interests, such activities should not be*

[1] General comment No. 25 (2021) on children's rights in relation to the digital environment, §12-13, p2-3.

undertaken". Such a statement however conflicts with §33 which states that: "*the purpose of the balancing exercise is not to avoid any impact on the interests and rights of the data subjects altogether. Rather, its purpose is to avoid a disproportionate impact and to assess the weight of these aspects in relation to each other."* The emphasis on protecting children does therefore not automatically prohibit the use of the legitimate interest basis in every situation but it merely requires the controller to consider a higher threshold regarding the data protection risks and the measures needed to contain them.

17. Furthermore, a controller needs to consider that the age and maturity of the child may affect the balance as well, whereby older children are less likely to be disproportionately impacted. We therefore cannot agree with the position that an organisation's legitimate interest will always be overridden when data of any child under the age of 18 is processed, as the organisation may be able to demonstrate that, taking account of the child's age and maturity such processing has a minimal or no effect at all on the interests or fundamental rights and freedoms of the child or that it can even be mutually beneficial for both parties.

Processing for the purpose of preventing fraud

18. Recital 47 GDPR confirms that "*the processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned*." The Guidelines however erroneously quote this text of the recital in §100, indicating that it clarifies that such processing *"may"* constitute a legitimate interest of the controller. We call on the EDPB to rectify this statement.

19. As mentioned above, our sector faces numerous cybersecurity threats that may not only compromise the integrity of a video game service and that of the terminal equipment of its users, but also any personal data that is processed in these environments. Video game companies have therefore adopted various proactive security measures that aim to detect hacking attempts, prevent fraudulent behaviour, protect players and maintain a secure gaming environment. Video Games Europe welcomes that the Guidelines in §104 explicitly recognise that the detection of fraud can, in principle, also be considered to be covered by the concept of "fraud prevention".

20. Indeed, requiring consent in fraud detection scenarios would be both impractical and ineffective, as malicious actors would simply decline to provide it. Consent is particularly not suitable for individuals who have already committed fraud against a controller in the past (consent can hardly be obtained from fraudsters). Also, for fraud detection to function well, it is necessary for providers to be able to draw trends, patterns, and insights based on a sufficiently representative sample of users; such representative sample can never be obtained by consent alone.

21. We are however concerned with the requirement in §105 that "*controllers should be specific about what type of fraud they are trying to prevent, and what data they really need to process in order to prevent that type of fraud".* The provision of that type of

information as part of a balancing test which, as suggested in §68, would be accessible to the data subject on request, could reveal knowledge regarding the technical operation of propriety detection methods and allow bad actors to make changes in order to go undetected in the future. Such information should, therefore, be regarded as a trade secret, the sharing of which would potentially defeat the purpose of the processing and lead to worse outcomes for data subjects.

22. Furthermore, as hacking into video game software may also compromise the safety and security of the personal data of other players, companies are under a legal obligation as controllers to implement appropriate measures to contain this risk. Not disclosing this type of information should therefore be considered as a necessary and proportionate measure *"to prevent unauthorised access to or use of personal data and the equipment used for processing"* in order to ensure appropriate security and confidentiality, as explicitly required under Articles 5, 24 and 32, and Recital 39 of the GDPR.

23. We also regret that the EDPB seems to be narrowing the lawful bases for subsequent processing, and thereby deviates from its earlier opinions. Particularly, §115 of the draft guidelines states that: "[ ] *consent will likely constitute the appropriate legal basis both for storing and gaining access to information already stored on the user's device and for the subsequent processing of personal data, thus normally precluding reliance on Article 6(1)(f) in this context*." This deviates in our view from EDPB's earlier opinion 5/2019, which states in paragraph 75 that: "[ ], *data protection authorities remain fully competent to assess the lawfulness of all other processing operations that follow the storing of or access to information in the terminal device of the end-user.* "

Processing for direct marketing purposes

24. The Guidelines indicate in §113 that controllers who engage in the processing of personal data for direct marketing purposes should also take account of the ePrivacy Directive, which requires that the sending of unsolicited communications for purposes of direct marketing by email, SMS, MMS and other kinds of similar applications can only take place with the prior consent of the individual recipient". As it is unclear what "other kinds of similar applications" actually means, footnote 137 further explains that the list of means of communication is not exhaustive. In this context, reference is made to §38-39 of the CJEU ruling in **StWL Städtische Werke Lauf a.d. Pegnitz** (Case C-102/20). This ruling however merely states that "*it is necessary to adopt an interpretation that is broad, and evolving from a technological perspective, of the types of communication covered by that directive*". We would like to receive further clarification on the applications that would be subject to this requirement.

25. The Guidelines explain in §119 that controllers should ascertain "*whether the marketing interest pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental freedoms and rights of the data subjects*". As it is unclear to us whether there are any other means that are just as effective as direct marketing and that can be applied to pursue the same marketing purpose, we would also like to receive further clarification on this point.

About VIDEO GAMES EUROPE

26. Since 1998, Video Games Europe has ensured that the voice of a responsible 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. Video Games Europe represents 19 European and international video game companies and 13 national trade associations across the continent. Europe's video games sector is worth €24.5bn, and 53% of Europeans are video game players. We publish a yearly Key Facts report with the latest data on Europe's video games sector.

VIDEO GAMES EUROPE Secretariat, November 2024