EUROPE'S VIDEO GAMES INDUSTRY

European Games Developer Federation

Joint ISFE-EGDF Reply to the Public Consultation on the EDPB's Guidelines 01/22 on Data Subject Rights – Right of Access

1. ISFE and EGDF welcome the opportunity to provide comments on the draft Guidelines 01/22 on the Right of Access by the European Data Protection Board (EDPB). Our members welcome the issue 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. The GDPR substantially widened the regulatory framework on the protection of personal data, in particular with new transparency requirements and data subject rights. These Guidelines will, therefore, be of great value to our sector and will help companies to deal with access requests from data subjects and to provide them with sufficient, transparent and easily accessible information about the processing of their personal data.

3. We have, however, 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 that hinder, rather than support, a meaningful implementation of the rules. 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:
    a. Data controllers should be given clear discretion to assess and deny requests where malicious intent is apparent. The Guidance creates uncertainty on this point through contradictory statements.

    b. The Guidance should give certainty to data controllers that, where they have provided an official and easily accessible route for the submission of data access requests, they may require its use for all such requests.

    c. Data controllers should be given further discretion about how they provide data, so that they can comply with the Article 12 requirement to provide data in a concise, transparent, intelligible and easily accessible form.

    d. The example relating to video games and anti-cheating practices in paragraph 171 should be clarified to ensure that games companies can fully protect both their own security and the rights of others, including players and themselves.

EXECUTIVE SUMMARY

4. The Executive Summary explains that there are no further exemptions or derogations other than the ones that the GDPR allows for. It is then stated that *"the right of access is without any general reservation to proportionality with regard to the efforts the controller has to take to comply with the data subject´s request."* Such a statement does not seem to align with Recital 4 of the GDPR which provides that *"the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."* Furthermore, the principle of proportionality is referenced repeatedly in the document, including in chapter VI on limits and restrictions where it states that *"the exercise of the right of access has to be balanced against other fundamental rights in accordance with the principle of proportionality."* The outcome of assessing whether an access request will have adverse (negative) effects on other participants' rights and freedoms will also have an impact on the efforts a controller must take to comply with the request.

5. We recommend using this executive summary to highlight the clear requirement in the GDPR to balance data protection with other fundamental rights and with the rights of others, as reflected throughout the rest of the guidance.

AIM OF THE RIGHT OF ACCESS, STRUCTURE OF ARTICLE 15 GDPR AND GENERAL PRINCIPLES

Aim of the right of access (§13)

6. We would ask the EDPB to reconcile an apparent contradiction between paragraph 188, which allows for malicious requests to be found as excessive, and Paragraph 13 which prohibits an evaluation of the motivation of the data subject. Our member companies need to be able to exercise discretion to assess and deny requests where malicious intent is apparent. Such requests are sadly frequent.

7. The Guidelines explain that controllers should not assess *"why"* the data subject is requesting access, but only *"what"* the data subject is requesting, and that the controller should not deny access on the grounds or on the suspicion that the requested data could be used by the data subject to defend themselves in court in the event of a dismissal or a commercial dispute with the controller. This would of course be without prejudice to any applicable national procedural rules adopted in accordance with Article 23 of the GDPR, which may determine for example the boundaries of the information to be provided, as explained in footnote 7.

8. The right of access should not apply to requests in which the data subject makes it sufficiently clear that they have a malicious intent. Video games companies, for instance, are regularly the victims of individual or coordinated actions by players seeking to use the right of access to apply pressure on companies to either reverse

decisions made by them to enforce their terms, or to use the data obtained through the right of access to attack the integrity of the companies' systems and/or to improperly obtain information that would be used in litigation against them. The Guidelines should make it clear that such requests should not be considered as lawful requests for access to data under Article 15 of the GDPR, in line with the position taken in paragraph 188. Controllers should therefore be provided with ample discretion in such instances to assess and deny requests where malicious intent is apparent.

GENERAL CONSIDERATIONS REGARDING THE ASSESSMENT OF ACCESS REQUESTS

Form of the data access request (§55)

9. Where a data controller has established a reasonable process through which a right of access can be exercised, it should be presumed compliant. The Guidelines should further indicate that only the official communication channel should be used to make data access requests, where such a channel has been provided. It is unreasonable to expect a controller to train every consumer-facing employee regarding how to properly process these requests when proper procedures can easily be established.

10. The Guidelines explain that a controller is not obliged to act on a request sent to the e-mail address of a controller's employee who may not be involved in the processing of requests concerning data subjects' rights. This position is then weakened by stating that such a request can be sent to any email address of any employee who deals with the data subject's affairs on a daily basis. The latter advice may be a cause for errors and should be rectified in the text. Emails might get lost when addresses other than the official one for data access requests are used. Emails of employees may be subject to stricter spam filters that could treat general access requests as spam or subject to less stringent deletion/retention schedules when the data is not identified as a structured access request. Employees may also simply be on holiday.

11. Furthermore, an employee's email address may not be subject to the same security standards. The controller is always obliged to ensure a level of security appropriate to the risk of the processing and will take this into account when setting up the official email address for data access requests. For these reasons, the Guidelines should clearly indicate that only the official communication channel, as identified in the privacy policy, should be used to make such requests. In-game self-service tools, for instance, allow for a secure identification of the person making the access request and a quick automated delivery of his or her personal data.

Identification of the requesting person (§72-72)

12. The Guidelines explain that controllers do not need to introduce additional safeguards to prevent unauthorised access to services when individuals want to access the data contained in their own accounts, and that it would be disproportionate to request a

copy of an identity document in such a case. The risk for the security of personal data created by the use of an identity document as a part of the authentication process will, however, never outweigh the risk of unauthorised data access (hacking) which often leads to a complete loss of all of the user's data. This is especially true for competitive online multiplayer games, where participants sometimes attempt to "eliminate" competing players by obtaining unauthorised access to their game accounts. Data controllers are under a legal obligation to ensure appropriate security of personal data, including protection against unauthorised or unlawful processing (Article 5.1(f) GDPR). Verifying an identity document should be considered as a proportionate measure to ensure a sufficient level of security when there are serious doubts about the identity of the requesting person or serious indications of fraud, or where no other methods of verifying identity are available.

Exercise of the right of access on behalf of children (§83)

13. The Guidelines state that "*children are data subjects in their own right and, as such, the right of access belongs to the child. Depending on the maturity and capacity of the child, acting on behalf of the child by the holder of the parental responsibility could be needed.*" The EDPB should provide further guidance on how the assessment should be made regarding whether the right of access should be exercised on behalf of or directly by the child. It should also be clarified to what extent the age of consent should be taken into account in this context.

Requests made via third parties (§88-89)

14. Where third-party services (channels or portals) are used to make access requests, the controller must ensure that the service is acting legitimately on behalf of the data subject. This is because the making available of personal data to the data subject is a processing operation for which the controller is always obliged to ensure a level of security appropriate to the risk. Data security requirements apply independently of the modality in which access is provided and must be taken into account by the controller when choosing the means of transfer. Furthermore, it is recommended in paragraph 70 that the controller should implement an authentication procedure in order to be certain of the identity of the persons requesting access to their data and to ensure security of the processing throughout the process of handling an access or portability request.

15. However, in the context of third-party portals, the EDPB argues that, although controllers are under no obligation to provide the data directly to such a portal, access requests from these portals should, "*invariably*", be handled in a timely manner. This implies that controllers are required to engage with requests received by these third-party service providers. This requirement would pose security concerns as it is often impossible to verify with a sufficient level of certainty that the third-party service has the right to make such a request and to receive the data on behalf of the data subject. For example, the third party may require the controller to visit its portal and create an account to view an 'authorisation document'. Firstly, the controller should not be

expected to visit a third party's portal and secondly, the authorisation documents are not notarised Powers of Attorney. Accordingly, this puts into question the service provider's authority to act on behalf of the data subject. Further, the information provided by these portals/service providers rarely provides the information necessary to allow a controller to confirm the ownership of a player's account. This means that video game companies would need to reach out directly to the data subject and/or the third-party service to confirm such details, which is administratively burdensome. Requiring controllers to modify their own procedures to address such requests and engage with these service providers would impose an unreasonable administrative burden upon them as the requests are often mass automated requests that are not properly authorised by the data subjects. Furthermore, when companies do engage directly with data subjects with respect to the requests received from these third parties, much of the time they either do not receive a response or the data subject confirms that they do not wish to proceed. The Guidelines should, therefore, explicitly acknowledge that where controllers offer an easy and secure way to exercise their rights, they may rely on these mechanisms instead of engaging directly with such third-party service providers.

SCOPE OF THE RIGHT OF ACCESS AND THE PERSONAL DATA AND INFORMATION TO WHICH IT REFERS

Definition of personal data (§95)

16. The Guidelines state in reference to case C-434/16 of the Court of Justice of the European Union that written answers submitted by a candidate at a professional examination and any comments of an examiner with respect to those answers constitute personal data concerning the exam candidate. An example is then used in the context of a job interview to further specify that a controller needs to provide the data subject with a summary of the interview, including the subjective comments on the behaviour of the data subject that the HR officer wrote during the job interview. The EDPB should acknowledge that the limits resulting from Article 15.4 (rights and freedoms of others) requires vigilance that the provision of the personal notes of the HR officer may not lead to the disclosure of personal data related to other applicants.

Personal data concerning him or her (§104–105)

17. The EDPB considers that the words "*personal data concerning him or her*" should not be interpreted in an *"overly restrictive"* way by controllers. It is argued that recordings of telephone conversations (and their transcription) between a data subject who requests access and the controller may fall under the right of access provided that the former are personal data. The EDPB should acknowledge that the limits resulting from Article 15.4 (rights and freedoms of others) should be taken into account in such a case. Controllers may choose to implement additional measures to protect the rights and

security of the interlocutor on the side of the controller, for instance by blackening out their names on the transcripts.

18. Furthermore, the Guidelines state that, in case of identity theft, a victim who requests access to his data should be provided with information on *all* personal data the controller stored in connection with his identity, including those that have been collected on the basis of the fraudster's actions. However, providing such information could require the controller to grant access to another individual's personal data without appropriate authorisation which could constitute a personal data breach under the GDPR.

Information on the processing and on data subject rights (§110-120)

19. In addition to access to the personal data themselves, the controller has to provide information on the processing and on data subject rights according to Article 15(1)(a) to (h) and 15(2) GDPR. The EDPB considers that such information may only be communicated in general terms where it does not change depending on the person making the access request. The information on recipients, on the processing purpose, on categories, on the source of the data, on data retention, on data subject rights, on automated processing, and on international data transfers may therefore vary depending on who makes the request and what the scope of the request is. The EDPB argues that such information may have to be updated and tailored for the processing operations carried out with regard to the actual case of the data subject making the request.

20. Data controllers who receive a large numbers of access requests every day are unable to (manually) provide tailored information with regard to the specific case of each data subject and must revert to automated processes to ensure an efficient and timely handling of access requests within the legal timeframe. Such an approach is accepted and even recommended by the EDPB in paragraph 135 while referring to the practice example of a social media service. The Guidelines should explicitly acknowledge that the provision of general information as also done in the privacy notice would suffice in such situations.

HOW CAN A CONTROLLER PROVIDE ACCESS?

Providing access in a concise, transparent, intelligible and easily accessible form using clear and plain language (§138-141)

21. Data controllers should be allowed some discretion regarding the provision of all personal data that a user could reasonably expect based on an initial request. The guidance should ensure this by more clearly reflecting the requirement in Article 12(1) GDPR for a controller to take appropriate measures to provide data in a concise, transparent, intelligible and easily accessible form, using clear and plain language. We

agree with the EDPB that this also means that a controller should take into account the quantity and complexity of the data when choosing the means for providing access under Article 15.

22. This is illustrated in the Guidelines with an example from a social media service in which a large part of the requested data consists of hundreds of pages of log files. We agree that in such a case the controller must be careful and thorough when choosing the way the information and personal data is presented to the data subject. Data access requests in the video game sector may also cover large amounts of raw data related to the gameplay activity of the user in the video game. The provision of such information does not help to achieve the purpose of the right of access, which is to ensure the controller is processing personal data properly.

23. We also agree with the EDPB's assessment that there may be a tension between the amount of information the controller needs to provide data subjects and the requirement that it must be concise. The proposal to present in such circumstances the personal data and supplementary information in different layers is certainly helpful. Controllers should be allowed discretion to provide all personal data that a user could reasonably expect based on an initial request. If a user requests additional detailed information, the EDPB should recognise that the extraction of unusual raw data about a specific user requires significantly greater resources, effort and time as such data is often highly technical, not easily translated into a player-facing form, and not segregated based on user input. The EDPB should acknowledge that the provision of such data can be a resource-intensive task which may affect the controller's ability to provide the data within the currently prescribed timeframe. Some of the complexities necessarily involved with these requests include a detailed review to ensure the rights and freedoms of other parties are protected, such as confirming that disclosure would not adversely affect the security and integrity of a company's systems or its intellectual property rights.

24. Where the complexity of the access request requires them to do so, controllers should have the option to provide further data at a later stage where the user has specifically requested to have such access. Such an approach should also be considered as an appropriate measure to fulfil the requirements of Articles 15 and 12(1) GDPR. In the event that further highly technical and resource-intensive information is requested that is beyond what should be reasonably made available to confirm the appropriateness of the data processing, the EDPB should also recognise that such a request may be made maliciously. In that instance, companies should have the right to deny the request.

LIMITS AND RESTRICTIONS OF THE RIGHT OF ACCESS

Article 12(4) (§171)

25. The example given in this paragraph relating to the use of third-party software to cheat in a video game should be expanded to fully reflect the level of threat represented to the interests of the video game company, the maliciousness of the use of data, and the need to balance the rights and interests of other players affected by the cheating.

26. The Guidelines correctly acknowledge that the right to protection of personal data is not an absolute right and has to be balanced against other fundamental rights in accordance with the principle of proportionality. If complying with an access request would have adverse (negative) effects on other participants' rights and freedoms, the interests of all participants need to be weighed taking into account the specific circumstances of the case and, in particular, the likelihood and severity of the risks. The EDPB recommends that controllers should always try first to reconcile the conflicting rights, for example through the implementation of appropriate measures mitigating the risk. However, if it is impossible to find a solution of reconciliation, the EDPB accepts that controllers have to decide which of the conflicting rights and freedoms should prevail.

27. The recommended procedure is illustrated with an example from our sector. It involves a player who has been banned from a video game platform in line with their terms and conditions due to cheating by using third-party software and who has asked the platform for access to all personal data relating to him. The Guidelines correctly state that the trade secrets of the video game platform preclude the disclosure of the player's personal data because knowledge of the technical operation of the anti-cheat software could also allow the gamer to circumvent future anti-cheat or fraud detection methods.

28. However, it is then suggested that, in addition to providing general information about the processing for the purpose of cheat detection, the video game platform should also grant access to the information it has stored about the player's cheating activities which led to the ban *"in order for the data subject to verify that the data processing has been accurate".* The text of the Guidelines mentions here in particular: log overview, date and time of cheating, and detection of third-party software.

29. ISFE and EGDF strongly disagree with this interpretation of the rules. First, much of the data detailing a player's cheating activities could reveal knowledge regarding the technical operation of the anti-cheat software and must fall under the exception to the right of access under Article 15(4). Cheating is often specific to a particular game but can be broadly defined as any action that alters or interferes with the normal behaviour or rules of a game. Cheating may involve modification of a video game client, abuse of server APIs, interception of server-client messages, so-called 'sockpuppet' accounts (misleading uses of online identities), and more. Cheating deprives genuine players of an authentic and fair gameplay experience, for example, by allowing cheaters to 'level

up' faster than other players, disrupting the gameplay experience and hindering progression for genuine players. Cheating can provide players with easier access to in-game collectibles, for example, which could demotivate other players from earning or collecting them. Cheating also places an administrative and financial burden on games companies. As an example, automated tools used by cheaters require significantly more bandwidth than 'human' players, leading games companies to incur significant additional server costs. Cheating also creates negative player sentiment, which causes genuine players to disengage from games, leading to impacts on revenue.

30. Detection and subsequent blocking of a cheating account often (and sometimes automatically) leads to the creation of a new account while masking the identity of the device operating the hacking software. Disclosing the date and time of the cheating activity would reveal when detection was triggered and would allow the operator to circumvent the anti-cheat software in a subsequent attempt. Timestamped data with location information can reveal when a company is employing the use of 'honeypots' (security mechanisms to detect, deflect or counteract attacks), which is particularly useful for a cheater to understand in order to evade detection. Divulging logs risks cheaters being able to pool individual information together to improve game hacks or to launch a targeted attack. Providing specific timestamped data makes this process even easier for cheaters. Any disclosure of information related to the hacking activity of the third-party software could reveal specific information about the functioning of propriety detection methods and allow the user to make changes in order to go undetected in the future. Such information should, therefore, be regarded as a trade secret.

31. Secondly, the right of access is designed to enable *natural persons* to have control over their personal data. Cheating within video games is enabled by an illegal multi-billion-dollar industry of organisations that employ subscription business models to sell or rent third-party cheat software to individual players as well as to companies. The cheating ecosystem has established itself as a vertical industry whereby various professional organisations make use of unauthorised access to the game code to enrich themselves. Some companies, for instance, pay for access to download video game content illegally in order to sell it to players and make large profits. Such companies often operate in an organised crime environment and do not hesitate to engage in other criminal activities, such as the use of stolen credit cards and money laundering. To the extent that such accounts are operated by a company instead of an individual, the corresponding data does not refer to an identified or identifiable natural person and fall outside the material scope of the GDPR. In such cases, the right of access will not apply.

32. Finally, hacking into video game software may also compromise the safety and security of the personal data of other players which puts companies under a legal obligation as controllers to implement appropriate measures to contain this risk. Whilst the example in the Guidelines is helpful, it should go further to acknowledge that controllers have greater discretion to deny access to the personal data of players when it comes to their cheating activities. It should 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.

33. Even if details regarding a player's cheating activity are withheld, video game companies would still provide access to personal data that is not related to cheating activities or otherwise limited from access under Article 15(4), even where it involves a player that has engaged in such cheating activities. His ability to have control over his personal data *"to be aware of, and verify, the lawfulness of the processing"* (Recital 63) should therefore remain fully unaffected.

Article 12(5) (§184-188)

34. The Guidelines state that *"when it is possible to provide the information easily by electronic means or by remote access to a secure system, which means that complying with such requests actually doesn't strain the controller, it is unlikely that subsequent requests can be regarded as excessive".* It is unclear why the existence of a particular means of access would overrule the necessary assessment of "excessiveness" that needs to be carried out by the controller. Even where digital means of access do not strain the controller, excessive repetitive requests can still cause damage to the controller.

35. While the Guidelines state that "*a vast amount of time and effort to provide the information or the copy to the data subject cannot on its own render a request excessive"*, they admit that requests can be regarded as excessive where data subjects make use of the right of access with the only intent of causing damage or harm to the controller. The examples given in this context relate to individuals that explicitly state an intent to cause disruption and those that systematically send different requests to a controller as part of a campaign. As stated above, the EDPB should also acknowledge that requesting highly technical and resource-intensive information beyond what should be reasonably made available to confirm the appropriateness of the data processing and with the sole intention of causing disruption should also be considered as excessive and provide a sufficient ground to deny access.

36. Furthermore, paragraph 187 of the Guidelines which states that *a "request should not be regarded as excessive on the ground that the data subject intends to use the data to file further claims against the controller"* should be amended to take into account the fact that such a request may still be regarded as excessive in situations where the data subject uses the right of access with a malicious intent to attack the integrity of a company's systems and/or to improperly obtain information that would be used in litigation against the company.

About ISFE and EGDF

37. The Interactive Software Federation of Europe (ISFE) represents the video games industry in Europe and is based in Brussels, Belgium. Our membership comprises national trade associations across Europe which represent in turn thousands of developers and publishers at national level. ISFE also has as direct members the leading European and international video game companies, many of which have studios with a strong European footprint, that produce and publish interactive entertainment and educational software for use on personal computers, game consoles, portable devices, mobile phones and tablets.
    Transparency Register Identification Number: 20586492362-11

38. The European Games Developer Federation e.f. (EGDF) unites national trade associations representing game developer studios based in 19 European countries: Austria (PGDA), Belgium (FLEGA), Czechia (GDACZ), Denmark (Producentforeningen), Finland (Suomen pelinkehittäjät), France (SNJV), Germany (GAME), Italy (IIDEA), Lithuania (LZKA), Netherlands (DGA), Norway (Produsentforeningen), Poland (PGA), Romania (RGDA), Serbia (SGA), Spain (DEV), Sweden (Spelplan-ASGD), Slovakia (SGDA), Turkey (TOGED) and the United Kingdom (TIGA). Through its members, EGDF represents more than 2,500 game developer studios, most of them SMEs, employing over 40,000 people.
    Transparency Register Identification Number: 57235487137-80

39. The purpose of both EGDF and ISFE is to serve Europe's video games ecosystem by ensuring that the value of games is widely understood and to promote growth, skills, and innovation policies that are vital to strengthen the sector's contribution to Europe's digital future. The games industry represents one of Europe's most compelling economic success stories, relying on a strong IP framework, and is a rapidly growing segment of the creative industries. In 2020, the size of Europe's video games industry was €23.3 billion and registered a growth rate of 22% year on year in key European markets[1]. There are around 5,100 game developer studios and publishers in Europe, employing over 87,000 people.[2] Today, 50% of Europe's population aged 6-64 plays video games and 47% of the players are women.

ISFE and EGDF Secretariat, March 2022

[1] ISFE-EGDF Key Facts 2021 https://www.isfe.eu/isfe-key-facts/

[2] 2019 European Games Industry Insights report: http://www.egdf.eu/wp-content/uploads/2021/08/EGDF_report2021.pdf