EUROPE'S VIDEO GAMES INDUSTRY

European Games Developer Federation

Joint ISFE-EGDF Reply to the Public Consultation on the targeted update of the EDPB's Guidelines 9/2022 on Personal Data Breach Notification under GDPR.

1. ISFE and EGDF welcome the opportunity to provide comments on the targeted update of Guidelines 9/2022 on Personal Data Breach Notification by the European Data Protection Board (EDPB) (hereinafter, the "revised guidelines"), specifically regarding its paragraph 73.

2. As further explained below, it is our view that the proposed update would be a significant step back in the creation of a "solid framework for digital trust",[1] considering how it would negatively affect both data subjects' data protection rights and the pursuit of legitimate business activities by controllers and processors of personal information. Our assessment is in consideration of three primary factors, as better explained in the sections below:
    A. The timeliness and efficiency of data breach mitigation and reporting;
    B. The consistency of EU law application;
    C. The efficiency of public resources across the EEA.

3. We also wish to raise a proposal for the EDPB to draft a weighting matrix of the risks presented in the Guidelines.

BACKGROUND

4. The so-called "one-stop-shop" mechanism (article 56 GDPR) allows controllers with a main establishment in the EU to notify a single regulator in case of a notifiable data breach. Without an identifiable main establishment, the general rule applies: when experiencing a notifiable data breach affecting data subjects in multiple Member States, controllers need to notify every relevant supervisory authority (article 55 GDPR).

5. The *Article 29 Data Protection Working Party Guidelines on Personal data breach notification under Regulation 2016/679 (WP250rev.01)* (hereinafter, the "existing guidelines") provide guidance to avoid the consequences of applying the aforementioned general rule to controllers subject to article 3(2) who cannot rely on the "one-stop-shop". The recommendation is to only notify the "supervisory authority

[1] See The European Commission's "A European Strategy for Data", p. 4, available here.

in the Member State where the controller's representative in the EU is established" (p. 18).

6. The existing guidelines, in our opinion, serve as a stop-gap solution that is not otherwise addressed in the GDPR.

7. The existing guidelines' recommendation is appropriate as it helps address a number of issues that would arise in its absence, including:
    a. The obligation to address a data breach is urgent by nature. The need to notify up to 30 regulators (and consequently to engage in up to 30 different procedures) inevitably delays the entire process with considerable impact for every stakeholder, including data subjects.
    b. There is a single event to analyse (or a series of connected events, as also foreseen in paragraphs 63 and 64 of the revised guidelines). Having multiple supervisory authorities autonomously analysing the same facts would not only produce inconsistencies (and consequently potential discrimination to data subjects, as further explained below), but would also be a waste of public resources.

8. The existing guidelines address the above issues by providing:
    a. **An analogous mechanism** - The lead supervisory authority mechanism (article 56) provides a legal solution that can and should be adapted considering the urgent nature of the situation.
    b. **Simple criteria** - In the absence of a main establishment, the Member State where the representative is established is the simplest and therefore quickest way to determine a competent supervisory authority, which again is especially relevant considering the urgency of the matter.

THE CONSEQUENCES OF THE REVISED GUIDELINES

9. The revised guidelines strikingly propose to remove the aforementioned recommendation. ISFE and EGDF strongly oppose the proposed procedural change as it would create a considerable increase in bureaucratic burden which would negatively impact all stakeholders involved, most of all the rights and interests of the natural persons affected. In particular, we highlight three main negative impacts of this change:

A. Timeliness and efficiency of data breach mitigation and reporting

10. Considering how widespread user bases in our sector are, a controller subject to article 3(2) without a main establishment would typically need to notify most or all relevant supervisory authorities. This would require engaging in up to 30 different notification procedures, in different languages, which would then be followed by discrete interactions with such supervisory authorities.

11. Companies would need to significantly increase the amount of time, human and financial resources dedicated to data breach mitigation and reporting processes. However, even with increased resources, the reporting burden would impact companies' ability to take prompt remedial action and mitigate risks of damage to data subjects.

B. The consistency of EU law application

12. Without a streamlined cooperation mechanism in place to harmonise the application of the law across the EEA (such as the one foreseen in article 60 GDPR through the application of article 56 GDPR), each supervisory authority would be required to address the matter according to its best judgement.

13. This, however, will inevitably generate inconsistencies of outcomes depending on the jurisdiction concerned. A few examples in that regard:
    a. Some supervisory authorities may consider that data subjects need to be contacted, whilst others may not.
    b. Different remedies may be proposed to mitigate the matter.
    c. Different compensation may be prescribed to the data subjects affected.
    d. Different sanctions may apply to the same controller.

14. Such inconsistencies potentially result in discriminatory treatment for data subjects in relation to their data protection rights, since, e.g., a data subject in Spain may be offered a more thorough protection than a data subject in France, or vice versa.

15. The inconsistent treatment of controllers will no doubt have a negative impact on businesses who will be forced to operate in an unpredictable legal landscape.

C. The efficiency of public resources across the EEA

16. The proposed change not only creates an unreasonably high burden on controllers: it also exponentially increases the workload of national supervisory authorities. Many of them already reported in the European Commission's 2020 GDPR Application Report that they are lacking sufficient resources[2]. The report correctly identified that, besides impacting their capacity to enforce rules at national level, the increased workload also limits the national supervisory authorities' capacity to participate in and contribute to the cooperation and consistency mechanisms. The success of the one-stop-shop mechanism depends on the time and effort that data protection authorities can dedicate to the handling of and cooperation on individual cross-border cases.

17. The Commission's 2020 GDPR Application Report unveiled that there are significant discrepancies regarding notifications of a data breach between Member States, which points to a lack of consistent interpretation and implementation resulting in

[2] Two-Year Application Report of the GDPR – Commission Staff Working Document, p12-13.

differentiated treatment, despite the existence of EU-level guidelines[3]. Requiring controllers to notify the same breach to multiple instead of only one supervisory authority would lead to even less consistency in dealing with data breach notifications and less debate, cooperation and potential disagreement resolution between supervisory authorities. This would make the handling of cross-border cases less efficient and less harmonised across the EU.

Weighting Matrix Proposal

18. Finally, ISFE and EGDF members would like to take the opportunity of this public consultation to submit a business need. We would suggest to the EDPB to draft an "official" weighting matrix of the risks presented in the Guidelines 09/2022.

19. Reading the EDPB's Guidelines provides valuable advice in assessing the risks to data subjects in the event of a personal data breach. However, it would seem appropriate for the EDPB to accompany these theoretical guidelines with a practical matrix enabling an upstream assessment to be made of whether the risk to individuals is high, and whether notification to the supervisory authority should take place. Some paragraphs in the guidelines provide information to assist controllers in determining the risks. For instance, §75 states that "*An example might be where personal data are already publicly available and a disclosure of such data does not constitute a likely risk to the individua*l". The risk associated with this example could be a weight of 0 in the risk matrix. The higher the score of the matrix, the more the authorities should be notified in case of a breach.

CONCLUSION

20. ISFE and EGDF members support 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. However, we would like to caution that the proposed change in paragraph 73 would negatively impact the mechanisms that were adopted in the law to foster a uniform application of the data protection rules by ongoing cooperation and consistent interpretation. It would hamper the development of a truly common data protection culture between data protection authorities and lead to less, rather than more harmonisation. Furthermore, the change may also negatively impact the protection of natural persons with regard to the processing of their personal data which is one of the core objectives of the GDPR as stipulated in Article 1(1). We therefore strongly object to this procedural change and call on the EDPB to retain the procedure of the existing guidelines.

[3] Ibidem, p 11.

About ISFE and EGDF

1. 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

2. The European Games Developer Federation e.f. (EGDF) unites 22 national trade associations representing game developer studios based in 21 European countries: Austria (PGDA), Belgium (FLEGA), Croatia (CGDA), Czechia (GDACZ), Denmark (Producentforeningen), Finland (Suomen pelinkehittäjät), France (SNJV), Germany (GAME), Italy (IIDEA), Netherlands (DGA), Norway (Produsentforeningen), Poland (PGA), Portugal (APVP), Romania (RGDA), Serbia (SGA), Spain (DEV), Sweden (Spelplan-ASGD), Slovakia (SGDA), Switzerland (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 more than 40,000 people.
   Transparency Register Identification Number: 57235487137-80

3. 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. The European digital single market area is the third-largest market for video games globally. All in all, there are around 5,000 game developer studios and publishers in Europe, employing over 98,000 people. In 2021, Europe's video games industry was worth €23,3bn.[4]

ISFE and EGDF Secretariats, November 2022

[4] ISFE Key Facts from 2021 from GameTrack Data by Ipsos MORI and commissioned by ISFE.