MGIF Response to the European Data Protection Board's Consultation on the "Guidelines 01/2022 on Data Subject Rights – Right of Access"

Disclaimer: This paper does not represent the views of any single company, rather it is a sum of knowledge shared between MGI and Forum participants.

Introduction

On behalf of the Mobile Games Intelligence Forum (MGIF), it is a privilege to provide feedback to the European Data Protection Board (EDPB) on the updated Guidelines 01/2022 on data subject rights – Right of access. Our intention is to demonstrate the potential impact of these Guidelines on the mobile games sector – which generated around €10 billion in Europe in 2021, accounting for approximately 61% of all mobile app revenue in Europe.[1]

MGIF wholeheartedly supports the right of access according to data protection law. We believe it is vital to provide individuals with transparency and openness in terms of the processing of their personal data, whilst finding harmony in what information is useful to consumers and what is technically viable.

The scope of this response to the public consultation: Please note, we have limited our comments primarily to our mobile experience to provide a unique set of perspectives.

Forum Response: an in-depth reading of the draft guidelines

1. *"Proportionality"*

According to the Executive Summary, *"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."*[2] However, proportionality is mentioned multiple times in the document. For example, §171 - where it limits somehow the efforts the controller must take to respond:

"Hence also the exercise of the right of access has to be balanced against other fundamental rights in accordance with the principle of proportionality."[3]

It follows that our understanding is that proportionality remains a valid consideration in certain contexts under the Guidelines. We would support such a position and would value further clarification from the EDPB on this central issue.

2. 2.1. Aim of the right of access - §13

"Given the broad aim of the right of access, the aim of the right of access is not suitable to be analysed as a precondition for the exercise of the right of access by the controller as part of its assessment of access requests."[4]

[1] https://sensortower.com/blog/european-app-revenue-and-downloads-2021
[2] p.4
[3] p.50
[4] p.9

The Forum believes there are instances in which the denial of access to data is necessary. For instance, if the handing over of data will in some way be incriminating; or, if the motivation is to attack the integrity of our games and systems. Whilst a similar point on malicious intent is raised at §188,[5] when defining what constitutes an *"excessive"* request, it does not consider when an action is coordinated between multiple users. We respectfully suggest that such instances are factored into the Guidelines.

3. 3.1.2. Form of the request - §54-55

The Forum supports §54, interpreting it to mean that the controller does not have to act when a request is sent to the incorrect place, despite the appropriate communication channels having been provided. Nonetheless, this important and valid point is undermined in §55:

"However, if the data subject sends a request to the controller's employee who deals with the data subject's affairs on a daily basis (single contact of a customer, such as e.g. personal account manager), such contact should not to be considered as a random one and the controller should make all reasonable efforts, to handle such a request so that it can be redirected to the contact point and answered within the time limits provided for by the GDPR."[6]

We would respectfully suggest that only the official and secure way to make a request should be used. Emailing employees (including those using SAR[7]) should not be seen as a request, nor the starting point of the 30 days' timelines. Employees could be on holiday; the email could go into the wrong folder, the email may itself be considered as phishing. Therefore, it is a source of many potential errors, and, in turn, liabilities.

4. 3.3. Proportionality assessment regarding identification of the requesting person - §72-73

"Consequently, it is disproportionate to require a copy of an identity document in the event where the data subject making their requests are already authenticated by the controller."[8]

As a Forum, we advise that this sentence needs to be moderated. We have seen, on several occasions, account takeovers where the hacker requests data and deletion of the account; meaning that the legitimate player loses everything. The exception of national law in §73 may not be sufficient. Ergo, an appropriate caveat may be one that enables a company to verify identity if they have a serious suspicion of fraud, account takeover, or similar. For instance, it is suspicious when someone logs in from an IP address from a different country than they usually connect from.

5. 3.4.2 Exercising the right of access through portals / channels provided by a third party - §88-89

It should be clear that, when the controller offers an easy and secure way to make the request and access the data (at no cost), the controller should not be obliged to use the third-party service. Additionally, the Forum suggests that the mere reception of a third-party request should not be seen as the starting point of the 30-day timeline. As discussed, in reality, it is often difficult to verify that the proxy has the power to make the request and receive the data on behalf of the data subject. Furthermore, the information those proxies are sharing is often not relevant for us to authenticate and confirm the

[5] p.56
[6] p.22
[7] Subject Access Request
[8] p.25

ownership of the account. Another aspect that may be of value is that many proxy services try to push companies to open a business account on their platforms in order to action those SARs, and by doing so, force their own terms and conditions and privacy policies (which are often not up to GDPR standards as most of them are based outside of the EU).

§89: *"Under such circumstances, when the controller has other procedures in place to deal with access requests in an efficient way, the controller can provide the requested information through these procedures."*[9] Disclosing data to an unauthorised party is a risk and a personal data breach, as per §79.

6. 4.2.1. *"Personal data concerning him or her"* - §105

"Then again, there are situations in which the link between the data and several individuals may seem blurred to the controller, such as in the case of identity theft. In case of identity theft, a person fraudulently acts in the name of another person. In this context it is important to recall that the victim should be provided with information on all personal data the controller stored in connection with their identity, including those that have been collected on the basis of the fraudster's actions. In other words, even after the controller learned about the identity theft, personal data is associated with or related to the identity of the victim and therefore constitutes personal data of the data subject."[10]

The Forum reads this in a way that all information needs to be provided in case of an account takeover or a hack, because the data of the hacker is essentially attached to the legitimate account owner. Consequently, we would dutifully point out that this may be in contradiction of §46 and constitutes a data breach: "*As a general rule, a request may only concern the data of the person making the request. Access to other people's data can only be requested subject to appropriate authorisation."*[11]

7. 4.3. Information on the processing and on data subject rights - §111-112, §114

If teams are able to tailor the game/offers based on players' identifiers, then it follows that a player should be able to find out information on how the game was tailored for them. For instance, some gaming companies may exhibit a full list of advertising partners on their website, but not all partners are active in all games. So, when a player requests access, the company is in a position to tell them with what partners they have shared their AdID.[12]

Information on user data is disclosed in privacy policies and apply generally to all users. Mobile games that serve advertisements are not always able to follow the trail for each individual player to determine which advertisement(s) were serviced and therefore with which network(s) and/or publisher(s) data is shared, but the individual should be able to determine this for themselves.

8. 5.2.3. Providing access in a "concise, transparent, intelligible and easily accessible from using clear and plain language" - §139

"When providing data in a raw format it is important that the controller takes the necessary measures to ensure that the data subject understands the data, for example by providing an explanatory document that translates the raw format into a user-friendly form. Also, it could in such a document be explained

[9] p.29
[10] p.34
[11] p.19
[12] The advertising industry standard unique identifier for all commercial assets.

that abbreviations and other acronyms for example "A" means that the purchase has been interrupted and "B" means that the purchase has gone through."[13]

The purported requirement to not only provide access to but also *"explain"* raw data to the data subject seems entirely disproportionate. Providing access to such data is, in itself, a costly operation in terms of time and money (e.g., cost of processing power). Having to additionally explain each and every data point is an unfathomable burden. Furthermore, there are trade secret related concerns with providing such an *"explanatory document,"* since this would entail conferring detailed information on, for example, the analytics operations of the developer.

If a data subject asks for additional information on the meaning of one data point or another, then as a practical matter this can be arranged and, except in rare cases, we expect a controller would not have issue with providing a response. However, providing a comprehensive explanatory document covering all data to which access is given should not be an upfront requirement.

9. 5.2.4. A vast amount of information necessitates specific requirements on how the information is provided - §143-144

Following from our previous point, §143-144, as we understand it, may need some further clarification. Segmentation is integral to our games and may reveal information about the inner workings of the game that constitute trade secrets and/or competitive advantage. As an industry, unlike, for example, online retailers or video streaming sites, we do not generally know things like player age, gender, etc., on an individual level - segmentation is based on in-game activity. Thus, it is likely that we would not want to reveal which type(s) of activity and/or what frequency and/or timing of activity are considered. As such, if we are required to reveal the raw data (log-in, time-in-session, purchases made, coins won, spin used, etc.), we would not want to also reveal how we use that data to enhance the gaming experience.

10. 6.2. Article 15(4) GDPR - §166-171

The Forum has a robust stance that the fight against cheating is a pertinent issue for game integrity and player retention. As such, disclosing data related to a banned player due to cheating is dangerous for the following reasons: Firstly, it can be used to reverse engineer a gaming company's anti-cheat system. Second, providing all data related to a ban would also help wrongdoers to improve cheat bots, for instance, by knowing the date and time of the detection, they could identify which script they were using. Third, vast amounts of technical data are used in this very complex detection; for that reason, any single piece of information may be useful to understand a company's processes. Finally, some information related to a ban is already communicated (e.g., game logs), whilst not necessarily being identified as "ban data." We feel that the point in question should be significantly reappraised considering the above.

About MGIF

The Mobile Games Intelligence Forum was established in January 2020 to discuss and debate issues facing the sector and its place within the global video games industry. Rather than a representative body or a trade group, MGIF is a European focused participatory Forum, sharing mobile games insight and perspectives. A range of developers of differing sizes participate in the Forum. They have in common a passion for mobile games.

[13] p.43