Transparency register number: 57235487137-80

18.11.2024

EGDF response on the EDPB Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

About EGDF

1. **The European Games Developer Federation e.f. (EGDF)**[1] unites 23 national trade associations representing game developer studios based in 22 European countries: Austria (PGDA), Belgium (FLEGA), Croatia (CGDA), Czechia (GDACZ), Denmark (Producentforeningen), Finland (Suomen pelinkehittäjät), France (SNJV), Germany (GAME), Italy (IIDEA), Lithuania (LZKA) Netherlands (DGA), Norway (Virke Produsentforeningen), Poland (PGA and IGFP), Portugal (APVP), Romania (RGDA), Serbia (SGA), Slovakia (SGDA), Spain (DEV), Sweden (Spelplan-ASGD), Switzerland (SGDA), Turkey (TOGED) and the United Kingdom (TIGA). Through its members, EGDF represents more than 2 500 game developer studios, most SMEs, employing more than 45 000 people.

2. **The games industry represents one of Europe's most compelling economic success stories.** Located at the crossroads of the ICT and cultural industries, the game industry is one of the rapidly growing segments of the cultural and creative industries. In 2021, there were around 5 500 game developer studios and publishers in the EU, employing over 85 000 people and running a combined turnover of over €18,3bn[2]. In 2022, Europe's video games market was worth €24,5bn, and the industry has registered a growth rate of 5% in key European markets[3]. The European digital single market is the third-largest video game market globally.

3. **A good player experience is based on game developer studios' ability to access player data.** Clarity on the scope of application of Article 5(3) of the ePrivacy Directive (ePD) is generally welcome, as technology has advanced significantly since the directive was drafted. Furthermore, nowadays, players expect a smooth user experience and personalised communication and services. The number of consents needed to fulfil regulatory obligations is constantly increasing, which raises the risk of a non-user-friendly consent tsunami, especially when a player starts to play a new game. Therefore, EDPB should carefully avoid over-extending the current directive's scope.

[1] For more information, please visit www.egdf.eu
[2] EGDF-ISFE 2021 European games industry insights report
https://www.egdf.eu/wp-content/uploads/2023/07/V9-VGE_EGDF-video-game-industry-report2021.pdf
[3] ISFE-EGDF 2022 Key Facts
https://www.videogameseurope.eu/news/europes-video-games-industry-publishes-2022-annual-key-facts-report-all-about-video-games/

EDPB guidelines should analyse the full Article 5(3) ePD, not just half of it

4. It is critical that the EDPB also include in its analysis the later half of Article 5(3): *"This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user."*

5. Consequently, the EDPB must add a new **"CRITERION E: the sole purpose of the operations carried out is NOT to carry out or facilitate the transmission of a communication over a communications network, or it is NOT strictly necessary in order to provide information society service explicitly requested by the subscriber or user "** to their guidelines under paragraph 6.

6. All technologies outlined in the draft guidance document can be utilised to deliver information society services as requested by the user. **It is imperative for the EDPB to acknowledge that according to the EU consumer law framework, it is not enough just to transmit the content or service; the content or service must comply with both the subjective and the objective requirements of conformity** as defined in articles 7 and 8 of Directive (EU) 2019/770 on digital contracts[4]. The EDPB should provide further guidance on how the requirements under ePrivacy directive and digital contracts directive should be balanced against each other.

7. In practice, this means that operations must protect the privacy of the users (as required by the GDPR and ePrivacy directive) and, according to the digital contract directive:

    - be of the description, quantity and quality, and possess the functionality, compatibility, interoperability and other features as required by the contract,
    - be fit for any particular purpose for which the consumer requires it,
    - be updated as stipulated by the contract,
    - be fit for the purposes for which digital content or digital services of the same type would normally be used, taking into account, where applicable, any existing Union and national law, technical standards or, in the absence of such technical standards, applicable sector-specific industry codes of conduct
    - be of the quantity and possess the qualities and performance features, including in relation to functionality, compatibility, accessibility, continuity and security, normal for digital content or digital services of the same type and which the consumer may reasonably expect, given the nature of the digital content or digital service and taking into account any public statement made by or on behalf of the trader

8. The operations allowed under the new Criterion E should include, for example, providing security features (identifying fraud) or implementing EU sanctions against Russia (blocking access to a service for Russian users).

[4] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770

The ePrivacy directive aims to protect the privacy of the users, not to prevent information processing.

9. As stated under Article 1 of the ePrivacy directive, underlined in its recitals 24 and 25 and acknowledged in the draft guidance document, the goal of Article 5(3) ePD is to protect the privacy of the users. Consequently, it is surprising that EDPB has not fully reflected, under chapter 2.2. of the draft guidance document, the relationship of article 5(3) to all the measures service providers take to anonymise the information. Instead, the EDPB just bluntly assumes that article 5(3) ePD applies to all information regardless of this impact on the privacy of the users.

10. When the information is rendered in a way that the original information stored on the device is no longer identifiable (through the application of hashing or a similar process), Article 5(3) ePD should not apply, as the underlying concern about revealing personal or non-personal information from an end-user's device is sufficiently mitigated. This should be the case even if the information is, after it has been rendered unidentifiable, temporarily stored (or cached) on the device to enable its transmission, and the information is used to create a unique identifier, as discussed in section 3.5 of the guidelines.

11. Consequently, EGDF welcomes the fact that EDPB clearly indicates (paragraph 43) that on-device processing is not subject to Article 5(3) ePD "*as long as the information does not leave the device*". However, the EDPB should further clarify that *"any derivation of this information, when accessed through a communication network, may only be subject to Article 5(3) if the derivative information can reasonably reveal information about the information stored on the device"*.

IP addresses are often connected with the routers, not with the user's terminal equipment.

12. EDPB should be careful not to over-extend the scope of ePrivacy regulation on cases that do not involve the use of information stored in the user's terminal equipment. **It is highly questionable if the scope of Article 5(3) ePD can widened as far as concluded in the draft guidance document**: " *While it is not systematically the case (for example, when CGNAT12 is activated), the static outbound IPv4 originating from a user's router would fall within that case, as well as IPV6 addresses since they are partly defined by the host.*"

13. First of all, it is essential to acknowledge that a router is not terminal equipment. Secondly, many routers are not defined by the host. Nowadays, telcos often deliver routers as plug-and-play that do not require any configuration by the users. Thirdly, multiple users often use a single IP address to which a router is connected.

14. Consequently, the fact that an IP address may be assigned to a device such as a router can not, as such, mean that obtaining an IP address in the course of receiving data packets from the end user's device is "gaining access to information already stored" on an end-user device. In essence, such an interpretation makes any information an entity receives potentially subject to Article 5(3) ePD, even when the entity has not accessed or attempted to access an end-user device. This is especially the case with IP addresses, as the transmission and the use of IP addresses are fundamental to internet traffic.

15. **Accordingly, the "gaining access" criterion should only be fulfilled when an entity has actively attempted to "gain" access to (information already stored on) an end-user device**. Collecting or receiving information without such an attempt (for example, passively operating a web server or other service) should not fall under Article 5(3) ePD.

16. Therefore, it is a good question whether the following advice in the guidance document is more a good practice than a legal requirement: *"Unless the entity can ensure that the IP address does not originate from the terminal equipment of a user or subscriber, it has to take all the steps pursuant to Article 5(3) ePD."*

For more information, please contact

Jari-Pekka Kaleva
Managing Director, EGDF

jari-pekka.kaleva@egdf.eu
+358 40 716 3640
www.egdf.eu