Transparency register number: 57235487137-80

21.12.2020

EGDF response on the EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

About EGDF

1. **The European Games Developer Federation e.f. (EGDF)**[1] unites national trade associations representing game developer studios based 19 European countries: Austria (PGDA), Belgium (FLEGA), Czechia (GDACZ), Denmark (Producentforeningen), Finland (Suomen pelinkehittäjät), France (SNJV), Germany (GAME), Italy (IIDEA), Malta (MVGSA), Netherlands (DGA), Norway (Produsentforeningen), Poland (PGA), Romania (RGDA), Serbia (SGA), Spain (DEV), Sweden (Spelplan-ASGD), Slovakia (SGDA), Turkey (TOGED) and the United Kingdom (TIGA). Altogether, through its members, EGDF represents more than 2 500 game developer studios, most of them SMEs, employing more than 35 000 people.
2. **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. European digital single market area is the third-largest market for video games globally. In 2019, Europe's video games market was worth €21bn, and the industry has registered a growth rate of 55% over the past five years in key European markets.[2] All in all, there are around 5000 game developer studios and publishers in Europe, employing closer to 80 000 people.[3]

[1] For more information, please visit www.egdf.eu

[2] ISFE Key Facts 2020 from GameTrack Data by Ipsos MORI and commissioned by ISFE https://www.isfe.eu/data-key-facts/

[3] European Games Industry in 2018: http://www.egdf.eu/wp-content/uploads/2020/08/European-Report-on-the-Game-Development-Industry-in-2018.pdf

In general

1. **The free flow of data between the EU and third countries is crucial for European game developer studios.** Regulatory obstacles on the free flow of data create significant market access barriers for European SMEs operating in global digital markets, and it will adversely impact anyone working in Europe's digital economy.

2. **Government officials and policymakers in third countries, in particular in the UK and the USA, and in the EU need to act quickly to build a new, more reliable framework for data transfers** securing high standards on privacy and enabling the much-needed digital growth. As EDPB recommendations demonstrate, the absence of a stable international framework leads to significant administrative burden and legal uncertainty.

3. **The Commission should create a privacy-friendly regulatory framework for B2B contract terms.** The EDPB recommendations are written based on the assumption that B2B contacts are negotiated between two equal parties. In reality, global digital giants usually dictate the terms to European SMEs. Consequently, while the Commission is developing further the regulation of unfair B2B contract terms, it should carefully examine any contract terms conflicting with supplementary contractual measures listed in paragraphs 92-121.

Map of destinations

4. **The games industry is a global business.** First of all, as the games industry is a global business, industry representatives are constantly travelling around the globe and often need to be able to access the company data infrastructure from anywhere on earth. Secondly, as an outcome of the COVID19 pandemic, remote work from third countries is going to become far more normal. Furthermore, the games industry is an excellent example of an industry suffering from an acute talent shortage. This means that even small European game developer studios often have to hire external subcontractors from third countries.

5. **The EDPB should focus on security measures instead of regional data access limitations:** In paragraphs 12-13, the recommendation document notes that data controllers should contractually limit the remote access to the data (by data processors) to a limited list of destinations (map of destinations). Instead of limiting data access to specific counties, the recommendation document should focus on securing that sufficient security measures are always applied to data access from third countries.

Clear examples of high-risk and low-risk data

6. **Not all data is equally sensitive.** Low-risk data include, for example, time a player has played a game or the job titles of employees.

7. **The Recommendation document should take a more risk-based approach** and note that one part of the assessment should be to identify high-risk data that intelligence services or local authorities in third countries are more interested in (e.g. location data). Transferring data of this kind is both riskier and potentially harmful for data subjects than other types of data.

Assessment requirements

8. **European SMEs rarely have sufficient resources to case-by-case map and analyse laws and practices undermining their users' privacy globally.** However, the Recommendation document underlines that each data exporter should *"determine how the domestic legal order of the country to which data is transferred (or onward transferred) applies to these transfers*" (paragraph 32). Consequently, EDPB should:

    - Provide an exemption from burdensome transfer assessment process for low-risk data
    - Provide a list of high-risk countries whose surveillance laws and practices are not adequate. the Commission should use its vast embassy network all over the world to track privacy eroding changes in the local regulatory framework and make this information easily accessible for European SMEs. There must be a trustworthy source for European SMEs to double-check the information data importers provide on their local regulatory framework and its risks.
    - Create a single approved database of adequacy assessments
    - Expressly acknowledge that the requirement to assess an organisation's onward transfers can be met through contractual obligations on importers/processors / sub-processors to perform these assessments and that these recipients can, in turn, rely on their sub-processors' assessment. This would work the same way as exporters/controllers currently rely on the commitments of their importers/processors to conduct due diligence and impose the same level of security on their sub-processors. It is not feasible for SMEs to conduct assessments all the way down the supply chain of their service providers.

Objective factors

9. **Companies often have objective statistics about public authorities in different third countries requesting access to their data.** Therefore the Recommendations should not classify these statistics as subjective: *"you should look into other relevant and objective factors, and not rely on subjective factors such as the likelihood of public authorities' access to your data." (Paragraph 42).*

EU-USA data transfers

10. **In order to bring legal certainty on international data transfers, EDPB must also publish country-specific recommendations.** For example, the Recommendations indicate that US data importers subject to FISA 702 may be under an obligation to turn over any personal data in their possession, including access to cryptographic keys (paragraph 72). The EDPB appears to be implicitly

stating that there is no circumstance in which a US data importer subject to FISA 702 would be able to receive EU personal data. This also suggests that transfers to US data importers not subject to FISA 702 could be permissible if the appropriate safeguards are observed. It would be helpful if this was made explicit. The EDPB should also offer clear guidance stating that a company may comply by avoiding transfer of data for the part of its business that could be subject to FISA 702 and observing adequate safeguards (such as encryption) for those parts of its business that may not be subject to FISA 702.

The Recommendations should set conditions for the use of encryption that are workable in practice.

11. **Use cases 1 and 3 set unrealistically high conditions for sufficient supplementary encryption solutions:**

    - **Private companies do not have means to assess capabilities of foreign intelligence agencies:** According to the Recommendations these use cases require information to be encrypted using technology that *"can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them." (Paragraphs 79 and 84).* The capabilities of different foreign intelligence agencies to perform cryptoanalysis is not public information, and any public information is often based on rumours. Consequently, it is impossible for businesses to make evaluations of this kind.

    - **Unrealistically high encryption requirements will hinder access to necessary B2B services:** European companies rely increasingly on, often US-based, Software-as-a-Service (SaaS) like company email, payment processing, and document storage, customer relationship management, customer support, analytics, user testing, background checking services etc. Often these services need to have some remote access to clear data in order to provide their services. Consequently, too high encryption requirements may take away the utility of the data and prevents necessary data processing activities by the recipient. For example, it is necessary for central functions and relevant group companies to be able to access data held in shared systems in clear text.

12. **The EDPB should further clarify the relationship between use case 1 and 6.** Currently, the Recommendations can be understood to imply that data can be moved to an inadequate country if cryptographic keys are stored in the EU and not transferred to a third country (Use case 1), but data could not be moved at all to an inadequate third country if the cryptographic keys would be transferred to the third country for data processing (use case 6). In practice, this would lead to a situation where data would be moved to Europe for processing and then moved back to a third country as encrypted data. However, if the local regulation in the third country does not allow moving personal data to third countries for processing, the EDPB approach would potentially create a significant barrier for global digital trade.

13. **The approach recommended in the use cases 6 and 7, would significantly hinder global data transfers inside company groups.** Furthermore, they would require data localisation in the EU, which would make 24/7 customer support models difficult as assistance could not be anymore provided by teams based on different time zones. Furthermore, as aforementioned, it is crucial to keep in mind that as an outcome of the COVID19 outbreak, SMEs will increasingly rely on remote work. Therefore it will not be just global megacorporations that will have employees working for them outside EU, also European SMEs will have remote employees in third countries. It is likely that, in the future, SMEs will increasingly scale up their activities by having employees or subcontractors all over the globe. Already now Group subsidiaries rely on central systems infrastructure and services procured by the parent company/head office and managed and supported by specialised teams, which might be located at the parent company/head office (e.g. HR, Centralised Information Security systems, IT systems, privacy management systems that are hosted, supported, managed and accessed by a specialist team) using SaaS vendors.

14. **Consequently, the Recommendations should provide solutions that would qualify as supplementary measures for the use of central systems and services in global organisations.**

Additional contractual measures

15. **EGDF welcomes the list of additional contractual measures to complement and reinforce privacy safeguards** and hopes that EDPB will keep it constantly updated when new contractual measures are identified. Furthermore, the EDPB should underline that the mere fact that a contractual party located in third- country refuses to implement these measures should be considered a potential warning sign.

The Recommendations should provide for a grace period to implement these requirements.

16. **Both Schrems II ruling and the proposed Recommendations have created and will be creating a significant new administrative burden for European SMEs.** Beyond new contractual arrangments, European SMEs operating in the digital markets are forced to update their data infrastructure and workflows. Furthermore, this work is often relying on third-party service providers acting as processors or joint controllers for these SMEs. Therefore the Recommendations should define a grace period, aligned with the one offered for Standard Contractual Clauses, which would allow organisations to find acceptable solutions and have sufficient time to implement them.

For more information, please contact

Jari-Pekka Kaleva

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