EUROPE'S
VIDEO GAMES
INDUSTRY

ISFE Comments on the EDPB's Recommendations 01/20 on Supplementary Measures for International Data Transfers – Public Consultation

Transparency Register Identification Number: 20586492362-11

1. The Interactive Software Federation of Europe (ISFE) represents the European video games industry. ISFE's membership comprises national trade associations in 15 countries throughout Europe which represent in turn hundreds of games companies at national level. ISFE also has as direct members the leading European and international publishers, 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 the Internet.

2. ISFE welcomes the opportunity to provide comments on the draft Recommendations 01/20 on Supplementary Measures for International Data Transfers by the European Data Protection Board (EDPB). The video games industry is an international business, and many video game companies are offering their services globally. Companies are only able to deliver their services to their customers if they are in a position to process user data from around the world.

3. Video games companies depend on a reliable legal framework which allows to transfer the required data securely. They do not only need predictable rules to conduct everyday business operations, but also to make long-term decisions to invest and/or hire people. The CJEU ruling[1] "Schrems II" has created great uncertainty in this respect. A large number of the companies that relied on the Privacy Shield to conduct business in the US are European. This is particularly true for the many successful European mobile video game developers and publishers which serves a global market. Commercial data flows to the US, which are valued at approximately 1.3 trillion U.S. dollars annually, provide significant economic benefits to the EU economy.

4. The "Schrems II" ruling has also casted doubt on the validity of Standard Contractual Clauses and Binding Corporate Rules if they are used for transfers to countries that do not meet the threshold of the ruling. This may create complete disruption of all data

[1] Court of Justice of the EU (CJEU) *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (Case C-311/18, "*Schrems II*").

INTERACTIVE SOFTWARE FEDERATION OF EUROPE aisbl.
Rue Guimard 15 | 1040 Brussels | Belgium
T +32 2 612 17 78 | info@isfe.eu | www.isfe.eu

flows between EU and US economies and potentially also between the EU and other territories. The risk of substantial economic damage, in particular at a time when economic growth is fragile due to COVID, is very high. The ruling also creates uncertainty for third countries that have been, or are in the process of being, granted 'adequacy' status by the European Commission. It will seriously discourage other countries, including the UK, from seeking to apply for such a status.

5. It is therefore of utmost importance that the EDPB provides practical and clear guidance to help companies comply with the Court's decision. The Recommendations have however adopted a prescriptive, non-risk-based approach that is contrary to the one taken by the GDPR and that goes well beyond the requirements of Schrems II. This does not follow the Court's instruction to take the context of a transfer into account. The Recommendations impose burdensome obligations on organisations to carry out detailed transfer assessments regardless of the risk and rely too much on encryption above other measures. The overall effect is that they do not provide any comfort for most transfers and risk making it impossible for organisations to comply with GDPR while carrying out everyday business activities.

6. ISFE would like to highlight the following issues in the text of the Recommendations that are both unrealistic and disproportionate and create serious obstacles for any organisation that is engaged in the transfer of personal data outside the EU. Failure to address these, risk isolating European companies from the global digital economy which will negatively impact European competitiveness and innovation.

The EDPB should permit processors and sub-processors to manage the location of their services.

7. As a first step, the Recommendations require a data exporter to construct a "map of destinations" (paragraph 12) where its data may be stored or accessed, including by its processors and their sub-processors. This is to ensure that a data exporter knows where the exported personal data will be located and processed. It is however not practical for data exporters and processors to comply with this requirement. Data processors require flexibility in the geographic location of their facilities and staff who access them. They will not be willing to contractually commit to a certain set of locations for a particular customer at one point in time and update such locations if change is required. For example, as workforces are becoming increasingly global and mobile, a processor should not be expected to update all of its customers if it hires a new staff person in another country who may have access to a database containing its customers' information. Instead, that processor should have the independent responsibility to ensure that the location of that new staff person provides for sufficient security.

The Recommendations' step 3 assessment requirements are too burdensome for exporting organisations.

8. EDPB would require each data exporter to "determine how the domestic legal order of the country to which data is transferred (or onward transferred) applies to these transfers" (paragraph 32) and suggests broad resources (Annex 3) in which controllers could seek such information. It is unduly burdensome to place the onus on exporting organisations to evaluate the compatibility, and ongoing compatibility, of a third country's legal regime with being necessary and proportionate to a democratic society. In practice, most controllers do not have the resources or expertise to properly make these determinations. This will lead to differing and inconsistent conclusions on appropriate transfers and an increase in the compliance burden on organisations, with no real benefit to individuals.

9. The extensive assessments will slow down business processes and development due to increased review and documentation requirements. In order to help companies carrying out such complex assessments, ISFE would propose following changes:
   - Provide for an exception to the transfer assessment process for low-risk data.
   - Provide a list of countries whose surveillance laws and practices are not adequate.
   - Provide access to a single approved database of adequacy assessment.
   - 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 organisations to conduct assessments all the way down the supply chain of their service providers.

The Recommendations should set out clear examples of what is likely to constitute high risk data and what is likely to constitute low risk data.

10. A wide range of information would be captured by the definition of personal data under GDPR including a lot of low risk data. Business administration data such as a person's name, job title, business e-mail address and business phone number is likely to be considered low risk data. Contractual and organisational measures would be sufficient to protect this type of data. Employee data is commonly shared amongst global businesses particularly when reporting lines are to management in the US. Although this range of data varies with sensitivity, it should be protected in all cases but not to the extent of preventing the use of shared systems.

11. The Recommendations reject a risk-based approach in favour of a rigid, "one-size-fits all" approach which effectively rules out any transfers of any type of personal data to the US or other third countries with surveillance laws that do not pass the very high EDPB standard, where the recipient is able to access the data in the clear. This is also inconsistent with the GDPR approach as well as with the European Commission's proposed Standard Contractual Clauses for transfers to third countries, which allow for a risk-based approach regarding public authority access to data.

The Recommendations should not inappropriately dismiss the likelihood of public authorities seeking to access to data.

12. Furthermore, the Recommendations should not dismiss as "subjective," a data exporter considering the "likelihood of public authorities' access to [their] data in a manner not in line with EU standards." (paragraph 42). Statistics related to attempts by public authorities to access specific types of data from data exporters/importers are an objective measure and should reasonably be allowed to be relied upon in determining the likelihood of such access in the future. It should not be dismissed as subjective.

The Recommendations should provide clear guidance regarding transfers to US-based controllers and processors

13. Since the EDPB's guidance will have significant effect on transfers from the EU to the US, it should expand upon and clarify its guidance for this situation. 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 made was explicit. The EDPB should also offer clear guidance 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.

14. Use cases 1 and 3 in the Recommendations refer to encryption at rest and encryption in transit as providing sufficient supplementary measures to protect EU personal data

from surveillance regimes of third countries, so long as numerous conditions are met. These measures are not workable for organisations. The conditions that must be met if an encryption solution is to be deemed sufficient are unrealistically high. Both 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." It is impossible for any private company to make this determination. It is not possible to assess what capabilities governments have, particularly large and well-resourced agencies.

15. Encryption is not always appropriate, particularly when it takes away the utility of the data and prevents necessary data processing activities by the recipient. Most SaaS (Software-as-a-Service) operators must have some remote access to clear data in order to provide their services. It is necessary for central functions and relevant group companies to be able to access data held in shared systems in clear text.

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

16. The Recommendations state that there are no technical measures that would qualify as supplementary measures for Use Case 6 (transfer to cloud service providers or other processors which require access to data in the clear) and Use Case 7 (remote access to data for shared business services including personnel services and customer communication) is concerning, as it makes the operating model for many global businesses non-compliant with GDPR. Cross border data transfers that occur daily for global organisations will be impacted. The effect of this is to require data localisation in the EU.

17. Group subsidiaries rely on central systems, infrastructure and services procured by the parent company/head office and managed and supported by specialised teams (centres of excellence), which might be located at the parent company/head office. These include:
    - A central human resources (HR) system that is hosted, supported, managed and accessed by specialist teams in the country where the parent company/head office is located. That central HR system will feed data to other HR systems, for example: learning management, performance appraisals, payroll/benefits management and absence management. It is common to use data from the HR system to facilitate a "Single Sign-On" process for other business systems that employees across the globe need to access on a daily basis, for example: email, travel and expense, ethics hotline/web portal, customer relationship

management, privacy management and employee benefits. These corporate systems are typically provided by vendors, a number of which are US companies using US-hosted systems or other offshore locations.

- Centralised Information Security systems, IT systems, privacy management systems that are hosted, supported, managed and accessed by specialist teams. Such systems facilitate "Single Sign-On" as well as have data stored with SaaS vendors.

18. Global SaaS providers mainly based in the US are used for corporate functions, such as company email, payment processing, and document storage, customer relationship management, customer support, analytics, user testing, background checking services, and so on. This allows organisations to benefit from the specialisation and expertise that companies do not have available in-house. Many have US based data storage and those who are based elsewhere, or those that offer EU hosting as an option typically have a range of sub-processors that are based in the US and other countries, and even a provider who hosts data in the EEA may need access for support reasons from the US or other third countries.

19. Under the Use Cases 6 and 7 in the Recommendations, 24/7 customer support models will no longer be possible. European organisations provide 24/7 support for their customers as well as internal employees who may need urgent assistance outside European office hours. This is only possible through global coverage models with teams around the world (often including the US) that respond to customers, open tickets and start with the resolution of the customer issue. This service can be provided by entities/teams within the same group of companies or by third parties. These entities will invariably need access to the personal data to engage with the customer and help resolve the issue. The alternative would be a restriction to customer support for business hours. Both options would put European companies at disadvantage compared to their global competitors.

20. Non-EU organisations will be deterred from expanding into Europe if they will be required to have a separate set of infrastructure for the company's EU presence. EU organisations will not be able to expand globally if they are not able to correspond with business contacts in those countries or exchange HR or business contact data with their offices in those countries. They will not be able to benefit from technologies and services provided by technology providers located outside of Europe. European organisations will therefore not be able to choose from the best or most economically priced global providers in the market. They will be limited to not only EU service providers but even more narrowly to only those European service providers that do not have any supporting group companies or subcontractors outside Europe.

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

21. The implementation of the Schrems II ruling is requiring organisations to conduct impact assessments targeting a variety of aspects of their data transfers. The necessary changes are not always limited to an update of the contractual arrangements, but often require more substantial changes in the data infrastructure, software applications or technical workflow. As this can be a complex task, the Recommendations should define a grace period which would allow organisations to work with supervisory authorities to find acceptable solutions and have sufficient time to implement them. Ideally, this grace period should be aligned with the one offered for Standard Contractual Clauses.

ISFE Secretariat, December 2020