Anitec-Assinform

RESPONSE TO CONSULTATION ON

DRAFT EDPB RECOMMENDATIONS BUILT ON SCHREMS II JUDGEMENT

Introduction

The EU General Data Protection Regulation ("GDPR") allows personal data to be transferred from the EU to third countries only under certain conditions including via Standard contractual clauses (SCCs) standards approved by the European Commission.

In July 2020, the EU Court of Justice in the Schrems case stated that parties transferring data from the EU ("data exporters") can use the SCCs only if they ensure that the transferred data will be protected to a standard that is "essentially equivalent" to that under EU law. The CJEU also held that where that was not possible using the SCCs alone—in particular, because public authorities in the third country could access the transferred data without appropriate protections—then the exporter would need to apply "additional safeguards" to protect the data.

The EDPB's Draft Recommendations build on the new judgement of the Court with the purpose on one hand to explain how an exporter should determine whether additional safeguards are required, and on the other to identify those safeguards, including technical, contractual, and organisational measures to protect data.
We believe the document issued by EDPB fundamentally misinterprets the requirements laid down in the Schrems II ruling and, if adopted, would create unjustifiable disruption to economic activity and everyday life. In mandating drastic measures for all data transfers it would in essence impede or severely hamper the conduct of business outside Europe, with no corresponding benefits in terms of data protection. In a nutshell the recommendations goes far beyond the statement of the Court.
European companies operating internationally have achieved strong levels of integration across their businesses and affiliates around the world. Such integration also relies on common tools used by affiliates across the globe for various purposes: human resources (HR) management, marketing and sales, information systems, engineering, operations, finance, etc.

The survey conducted by together with DigitalEurope and Businesseurope about the use of standard contractual clauses (SCCs) shows that only 9 per cent of companies based in Europe do not transfer any data outside the EU, while 75 per cent use SCCs to transfer data to more than one non-EU country simultaneously. The majority of these are European businesses. Last but not least; only 25 % is aware of Schrems II and even less among SMEs.

In this perspective we deem the recommendations to have a great impact on companies, the future of European growth and our ability to connect with and interact with global partners.
Here below please find our key messages and comments.

Step Three Assessment

ANITEC-ASSINFORM
Associazione Italiana per l'Information and Communication Technology
Tel. 02 00632801 - Fax. 02 00632824
C.F e P.I 10053550967

Sede e uffici di Milano:
Via San Maurilio,21 20123 Milano

Uffici di Roma:
Via Barberini 11 00187 Roma

segreteria@anitec-assinform.it www.anitec-assinform.it

- The third step provides to assess if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools one is relying on, in the context of a specific transfer.
  This provision takes up most of the draft Recommendations. However, along with the accompanying European Essential Guarantees (EEGs), it fails to provide concrete guidance for data exporters and importers. This section of the draft Recommendations reiterates the Schrems II findings in relation to US law, while the EEGs for the most part concern rulings from the Court of Justice of the European Union (CJEU) relating to Member State laws.
  It would be useful if the EDPB could provide more concrete guidance concerning at least those third countries where it deems that the EEG requirements are met, if any.
  Section 702 of the US Foreign Intelligence Surveillance Act (FISA) is the only foreign law that is explicitly considered as inadequate in the draft Recommendations. However, in considering only whether the data importer or any further recipient falls under FISA's overall scope, the draft Recommendations fail to consider the context of the data in scope, which is a significantly more limited data set than all personal data processed by a covered data importer. While these factors may not be conclusive to reach a general adequacy decision, they should be relevant when considering if and how third-country legislation applies to the transferred data in a specific situation. This absence of guidance is compounded by the globally applicability of the recommendations to all EU to rest of world transfers. The focus on the US distracts from the widespread impact these recommendations will have on Europe's connection to countries around the globe.

- The draft Recommendations offer a blanket statement that contractual and organisational measures will in themselves 'generally' not be sufficient and can only act as complements to technical measures in order to prevent access by third-country public authorities. The GDPR does not set out a hierarchy when it comes to these measures. In the context of certain transfers, under a proportionate and risk-based approach, these organisations and contractual measures could provide sufficient protections.
  Similarly, in assessing whether such public access is possible, the draft Recommendations stipulate that only 'relevant and objective factors' should be considered in addition to relevant legislation, excluding factors the draft Recommendations call 'subjective' such as the likelihood of actual access to the transferred data.
  That said we recommend adding to paragraph 33 that the likelihood of public authorities' access in the specific case of a transfer scenario can complement the other factors for assessing the risk of the transfer. Clarify paragraph 42 to set forth that, when legislations in third country may be lacking, likelihood of access cannot be used as the sole criteria to determine the risk but needs to be factored in the assessment.

- This reasoning underscores the draft Recommendations' assumption that all transfers must equally make access to the transferred data 'impossible or ineffective,' irrespective of the full circumstances surrounding the transfer, simply based on a theoretical possibility of unjustifiable interference by third-country public authorities.
  In line with this reasoning, all the examples of effective supplementary measures in the draft Recommendations describe scenarios where the transferred data is made completely illegible in the destination country – not only by public authorities but also by the data importer itself.
  The natural person, it must be concluded that the information, both in transit and at rest in the destination country, can genuinely be considered anonymous.
  Irrespective of this interpretation, the draft Recommendations render controller-to-controller transfers completely impossible. A controller in the destination country – for example, a non-EU subsidiary of an EU parent company – must be able to process the transferred data for its own purposes, but clearly cannot do so if it cannot access the data.

Step Four supplementary measures

- A fourth step is to identify and adopt supplementary measures that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence. This step is only necessary

if the assessment reveals that the third country legislation impinges on the effectiveness of the Article 46 GDPR transfer tool you are relying on or you intend to rely on in the context of ones transfer.

- The supplementary measures 'aim to preclude potentially infringing access by preventing the authorities from identifying the data subjects, inferring information about them, singling them out in another context, or associating the transferred data with other datasets they may possess that may contain, among other data, online identifiers provided by the devices, applications, tools and protocols used by data subjects in other contexts.'
- Not only does this interpretation have no basis in the Schrems II ruling, but it sets a bar that may well be completely impossible to meet. The draft Recommendations do not consider that, even in the case of end-to-end encrypted services, at least some metadata needs to be unencrypted to achieve the transfer. This will include connection information, session state, IP addresses or basic subscriber data.
- From this perspective, we submit that upon closer scrutiny not even the scenarios identified by the draft Recommendations as providing effective measures (use cases 1–5) would meet the draft Recommendations' standards.

Enforcement of the draft recommendations use case 7

- This scenario (use case 7) provides data transfers for business purposes, within a multinational group of companies or between different companies engaged in mutual economic activities such as HR data and communications with customers, which are routine transfers for any company operating outside the EU.
  In all these cases, the draft Recommendations stipulate that, simply because the data is available in the clear to the data importer, no effective technical measures exists and the transfer must hence not commence or be stopped. This scenario represents the predominant part of all data transfers outside the EU as well described in the survey conducted by Business Europe and DigitalEurope.
  The draft Recommendations would force all these companies to stop their data transfers to non-adequate countries, with repercussions on their business that could be dire.
  We can also outline that, many services used by companies in the EU, even with a significant impact on the subject of data security (eg. Website security screening), are provided mainly if not exclusively by companies that transfer data abroad and in particular in USA, as there aren't technically / economically comparable alternatives on the market, at least at the moment. Compliance with the current conditions set out in the draft would entail the obligation of U.E. companies to no longer use these services, with the paradoxical consequence of increasing data vulnerabilities.

  Moreover, analysing applicable laws in the third country will be difficult to implement. The detailed analysis which seems to be required by the ruling in light of the EDPB Recommendations goes beyond what can reasonably be expected from companies. For example, the analysis made by Advocate General Saugmandsgaard Øe in his opinion of December 2019, based on the thorough assessments of the Irish DPC and the Irish High Court, is not the type of exercise that can realistically be performed by a company, specifically SMEs, before they start processing data in third countries. This is especially true in light of the obligation to continuously monitor all relevant aspects of the transfer, which will impede swift provisioning of services, including, for example, simply updating databases that benefit from the cloud delivery models.

  We think that while the risk assessment needs to be performed before transfers take place, it should be possible to analyse the risk prior to commercializing/using a service, and not prior to each transfer. This is paramount to maintain the smooth delivery of cloud services.

Recommendation contrary to GDPR

- Accountability is a central principle of the GDPR. However, its application has a general nature that merely states that the controller shall be responsible for the other six general principles for the processing of personal data. As the draft Recommendations explain, remote access from a third country is also considered a data transfer. We therefore do not believe that interpreting third-country transfers primarily through the

accountability principle is at all useful. Rather, the general principle for third-country transfers is laid out in Art. 44, which provides that controllers and processors must comply with the conditions laid down in Chapter V GDPR in order not to undermine the GDPR's level of protection.

- The draft Recommendations also extend the data minimisation principle to require that third-country transfers be limited to what is 'adequate, relevant and limited to what is necessary in relation to the purposes for which [the data] is transferred to and processed in the third country.' This appears to imply that the GDPR imposes a duty to minimise transfers themselves, as opposed to the overall data processing.
  This interpretation has no basis in the GDPR. The data minimisation principle applies in relation to each processing purpose, but not in relation to every processing activity undertaken within such purpose, which may include third-country transfers.
    - Organisational measures such as ISO certifications are also certified mechanisms under GDPR and the global nature of these standards can efficiently help global businesses assess and comply with relevant privacy laws, particularly if the standard is updated to address specific issues such as local surveillance laws. In this perspective, we recommend to amend paragraph 48 taking into consideration that a holistic view and a risk assessment can lead to the result that contractual and organizational measures alone can sufficiently protect the data subject. Further, include a reference to contractual and organizational measures in paragraph 33.

Binding corporate rules and ad hoc clauses

The draft Recommendations repeat that the Schrems II ruling also applies to binding corporate rules (BCRs) and ad hoc contractual clauses.
We would like to outline that both BCRs and ad hoc clauses are adopted by the competent data protection authority (DPA), satisfying DPAs that their contractual safeguards can be complied with. As such, we urge the EDPB to provide clearer reassurance as to their continued validity and that no further re-assessment of adequacy is necessary.

Conclusions

As industry we endorse strong protections for personal data, including when data is transferred to third countries. At the same time, we have substantial concerns about some potential interpretations of the Draft Recommendations. The EU Charter and the GDPR provide important and valuable protections for personal data. Although some aspects of the EDPB's Draft Recommendations provide helpful guidance other aspects appear to go much further and suggest a range of unworkable measures that would have a serious impact on companies and-as a consequence- on the whole economic and even social system as detailed below.
Above all, we think the Draft Recommendations should be risk-based and proportionate in-line with GDPR and CJEU ruling. Cross-border transfers of personal data are an integral part of the day-to-day operations of most organisations in Europe and play an invisible but vital role in everyday life for EU citizens. Companies in a diverse range of sectors, including healthcare, transport, retail, and financial services, as well as public sector bodies, routinely rely on the SCCs and binding corporate rules ("BCRs") to transfer data. If the EDPB makes it difficult or impossible for organisations to rely on the SCCs (and other measures under GDPR Article 46), exporters will likely instead try to rely on the derogations in Article 49 of the GDPR (also applicable to extremely limited cases (given the respect of the principles of occasionality and necessity), or of practical application (consent)to transfer data. In contrast to the SCCs and similar mechanisms, the Article 49 derogations include very limited safeguards. Thus, the Draft Recommendations could leave EU data subjects with fewer protections than they have today
Moreover, we deem the Draft Recommendations doesn't reflect the importance of the specific circumstances of a transfer, however, instead, they suggest that organisations must adopt further safeguards any time there is even a theoretical possibility that data may be accessed. Because there is a theoretical possibility that data may be accessed almost any time a company uses the Internet to communicate with people outside the EU, or shares IT functionality with non-EU entities, this means additional safeguards will need to be employed in almost every business transaction—regardless of the risk of access.

Anitec-Assinform

We believe that If these recommendations are adopted as they are, they will have a disruptive impact on businesses, large and small, in all sectors. The Draft Recommendations, if adopted, will make many of these transfers much more expensive, and in some instances likely impossible, particularly for small and mid-size companies.
If this will be the scenario, the recommendations could even lead to conflicts with competing EU Interests when suggesting the implementation of technological measures to impede law enforcement and national security authorities access to data. The suggestion will impact all surveillance measures including those that may be compliant with EU law and include appropriate limits for necessity and proportionality.

If we contextualize the time we are living in, the Draft Recommendations will probably exacerbate the economic and health challenges Europe is already facing. Businesses across Europe are reeling from the impact of COVID; being able to engage in commerce with customers, suppliers, and partners outside the EU will be absolutely critical to their recovery. Policymakers should be wary of making it more difficult to access and do business in global markets, and of imposing burdens and costs on business with no clear benefit for EU consumers. It is difficult to quantify the potential compliance costs of the measures proposed by the EDPB, but they will unquestionably be significant, and they will impact a wide range of sectors. If adopted, the Draft Recommendations would also make it more difficult for European companies, researchers, and government organisations to collaborate with counterparts outside of Europe—collaboration that is critical for a range of important public goals, including tackling the COVID pandemic.
In a nutshell we think the purposes in principle of the recommendations are understandable, although we suggest:

- The Draft Recommendations should explicitly acknowledge that, in evaluating the need for additional safeguards, the data exporter can and should consider the specific circumstances of the transfer—including the likelihood, based on documented expert analysis, that third-country national security authorities will in fact access the data, the scale and frequency of the transfers, the type of recipient, the purpose of processing, the nature of the personal data transferred, and other relevant factors.

- Eliminate the Use Cases in Annex 2, and instead provide exporters with a toolbox of safeguards from which they can choose depending on the nature of the transfer. The proposed one-sized-fits-all approach to safeguards isn't workable, and it isn't necessary. Instead, the Draft Recommendations shouldn't identify a list of potential safeguards, but be clear that data exporters should be free to choose whatever safeguards they deem most appropriate based on the context of the transfer.

- clarify how a combination of safeguards (technical, contractual, and organisational) can be effective. In some cases, technical safeguards can be the most effective additional safeguard, for example to avoid covert surveillance under authorities such as the U.S. Executive Order 12333. In other cases, organisational safeguards can be effective, such as to challenge orders. And contractual safeguards can buttress these measures by imposing liability on data importers to comply. To the extent that the Draft Recommendations can be read to conflict with such an approach, they should be revised.

Anitec-Assinform is the Italian Information and Communication Technology Association.
Anitec-Assinform expresses the union of Italian digital high-tech companies of all sizes and specializations in the digital area. We are members of Confindustria and Founding members of Confindustria Digitale. At a European level we are members of DigitalEurope.

For more information, please contact Barbara.Carnevale@anitec-Assinform.it