大成 DENTONS

International Data Protection Day
Schrems II Source Kit

28 January 2020

In July 2020, the Court of Justice of the European Union invalidated the Privacy Shield, one of the main instruments for lawful transfer of personal data to the US, and introduced new conditions for transfers made outside the EU under the Standard Contractual Clauses. This is the Schrems II case which has affected all non-EU data importers, including service providers that receive personal data from the EU. If, in the course of your business, you transfer personal data you have received from EU/UK individuals to a non-EU/UK entity, such as a cloud service provider, you have to adopt a new level of diligence on data protection for each provider.

To mark international Data Protection Day 2021, our market-leading Privacy and Cybersecurity group is pleased to provide you with this **Schrems II Source Kit** to navigate your way through the key materials. Here you will find insights from the consultation submissions made by various organisations relating to the EDPB Guidance on Schrems II and the proposed new SCCs, and links to the key source materials.

KEY CONTACTS

Nick Graham
Partner, London
D +44 20 7320 6907
nick.graham@dentons.com

Simon Elliott
Partner, London
D +44 20 7246 7423
simon.elliott@dentons.com

Antonis Patrikios
Partner, London
D +44 20 7246 7798
antonis.patrikios@dentons.com

Monika Sobiecki
Senior Associate, London
D +44 20 7320 6342
monika.sobiecki@dentons.com

Hakki Can Yildiz
Senior Associate, London
D +44 20 7246 7327
HakkiCan.Yildiz@dentons.com

Chantal Bernier
Of Counsel, Ottawa
D +1 613 783 9684
chantal.bernier@dentons.com

Todd D. Daubert
Partner, Washington DC
D +1 202 408 6458
todd.daubert@dentons.com

Marc Elshof
Partner, Amsterdam
D +31 20 795 36 09
marc.elshof@dentons.com

Insights from submissions to EDPB recommendations and new SCCs

Topic/question	Issue	Selected comments from submissions
Whether the risk-based approach be permitted in the assessment of third country laws	The new SCCs permit a risk-based approach in assessing whether the laws of the destination country provide essential equivalence. Organisations can take into account subjective factors such as "*the specific circumstances of transfer, any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities*". However, the EDPB recommendations say that such subjective factors should not be considered in assessments.	The majority of the submissions (and all of the private organisations) favour a risk-based approach. The arguments put forward include: • In Schrems II, the CJEU states that organisations must make "case-by-case" assessments and that "all the circumstances" must be considered when determining whether transfers can take place. This indicates the CJEU's intention to permit a risk-based approach and organisations to take into account factors such as the relevance of the data to foreign governments and the frequency and likelihood of such agencies' access to the data. As a result, if the practical risks are low, the commenters argue that the supplemental measures organisations are expected to adopt should be appropriately narrowed. It is also argued that the risk-based approach is firmly established in EU primary law and case law – similar approaches to risk can be adopted by controllers in their selection of processors, in the performance of DPIAs, in determining the extent of breach reporting, in implementing data privacy by design etc. EDPB's recommendation that "subjective" considerations are irrelevant is out of line with the GDPR's risk-based framework. • In rejecting a risk-based approach, the draft recommendations set a higher standard for personal data exported to third countries than for data hosted within the EU. • Most US companies do not deal in data that is of any interest to US intelligence agencies (according to the White Paper published by various US public authorities) so a risk-based approach is sufficient for the protection of data. On the other hand, some commenters, particularly noyb, argue against a risk-based approach on the basis that: • risk-based approach is not a general principle applicable to all provisions of the GDPR and that this approach was pleaded in Schrems II and rejected by the CJEU; • taking into account relevant practical experiences (such as absence of prior instances of requests for disclosure) would be extremely difficult since access by public authorities is usually confidential and such an element is wholly a matter of the controller or processor to prove. In practice, most representatives of an organisation will also not know about secret surveillance within their own organisation. noyb also states in its comments to the new SCCs that it will closely monitor the developments e.g. any adoption of a risk-based approach and "take appropriate legal steps should the European Commission adopt such an approach and controllers actually rely on this approach".

EDPB's interpretation of the Schrems II judgment

Some argue that the way the EDPB interprets the Schrems II judgment is overly restrictive.

Almost all of the private organisations and business associations whose comments we have reviewed argue that the EDPB recommendations fail to provide businesses with a realistic way forward on international data transfers. In particular, use cases 6 and 7 under the technical measures section of the Recommendations – which relate to business arrangements such as use of cloud computing and accessing data for HR purposes from outside the EU – are considered by commenters effectively as a prohibition to transfer data to "non-adequate" jurisdictions when it is, at any point, "in the clear". According to these commenters, this may also have other unforeseen, wide-reaching consequences such as:

- obstruction of the flow of cyber threat information from the EU to the rest of the world (as organisations would have difficulty alerting EU authorities to malicious activity originating in the EU because they will not be able to transfer IP addresses);
- non-EU importers need access to data hosted even in EU data centres for various administrative purposes (e.g. trouble shooting, application maintenance, deployment of new software /an application). The administrative users of importers could technically be able to access data in the clear – EDPB's approach does not provide a solution for such access. It is argued that this effectively limits the number of providers with which EU organisations can contract, and may therefore create additional costs and affect the EU organisations' competitiveness.

At least one commenter (European Banking Federation) argued that language in the Recommendations such as "strongly encrypted", "robust against cryptoanalysis", and encryption algorithm which is "flawlessly implemented" for data exporters requires a standard higher than what is required under Article 32 GDPR.

Finally, some, such as the US Chamber of Commerce, also argue that the Recommendations rest on the assumption that international transfers are necessary for third country governments to access EU personal information – they argue that information in the EU can be accessed without the need for the data to flow to a third country.

Territorial/ jurisdictional scope of the SCCs	Some provisions of the new SCCs signal a shift in the interpretation of the concept of "transfer of data". These provisions may mean the SCCs would no longer be needed when personal data leaves the "geographical scope" of the EU, but when it leaves the "territorial scope" of application of GDPR.	While many private organisations welcome the approach, various commenters (including Christopher Kuner and noyb) argue this to be problematic because: • GDPR does not contain any provision on the basis of which this interpretation can be made; • the protection provided under Article 3(2) (territorial scope of the GDPR) and Chapter V (Article 46) (transfer of personal data to third countries) is not the same – Article 46 provides a higher standard of protection. When the GDPR applies to data processing under Article 3(2), it does so regardless of the level of protection and the standards that apply in the third country; • the approach would incentivise the online monitoring of EU individuals by non-EU organisations (as that would trigger the application of the GDPR, thereby relieving them from the requirement to enter into the new SCCs); and • the CJEU has not taken a "jurisdictional approach" in Schrems II, despite the fact that the GDPR was applied and the relevant transfer was "related" to the offering of a service to an EU data subject (noyb). The EDPB and the EDPS also requested the Commission to provide sufficient clarity to organisations "as to the situations where they can rely on [the] SCCs, and emphasise that situations involving transfers outside the EU should not be excluded".
Assessment of third country laws and challenging access requests	Many organisations stated that carrying out assessments of third country laws (i.e. whether the laws of the destination country do not exceed what is necessary and proportionate in a democratic society) and challenging access requests are prone to be problematic in practice.	Issues raised by commenters include the following: • It is difficult for private organisations with limited resources to conduct assessment of the public authorities' powers in third countries. • Shifting the responsibility of deciding on the essential equivalence of a third country legal regime from the public sector to the private sector would result in a lack of uniformity and legal uncertainty for exporters. • Exporters might come to different interpretations, creating potential risks / distortion of competition and differing protections for data subjects. • The European Commission should limit any assessment as to whether the new SCCs provide an adequate level of protection in relation to a specific data transfer in the specific circumstances at hand (and not require, for example, to assess whether a country respects "the essence of the fundamental rights and freedoms" (CIPL)). • Generally, EDPB Recommendations shift responsibility to assess third country laws and practices to the data exporter, while the new SCCs emphasise the role of data importers in carrying out such assessments – a conflict between two documents which needs resolving.

		Some commenters suggested the European Commission implement practical tools to help organisations carry out assessments (e.g. a platform to access: (i) third country laws and materials; and (ii) a record of entities which have been subject to access requests from their public authorities). With respect to challenging access requests, some commenters argue that the new SCCs contain provisions which suggest that organisations are expected systematically to exhaust all possible avenues to challenge a request from a public authority, even if the request appears perfectly legitimate. They argue that data importers should be able to review the legality of the request "to assess the reasonable merit of the case, to determine the most appropriate course of action and to take into account conflict with EU law, level of risk on individuals, cost and feasibility" (CIPL).
Practical difficulties and other issues (SCCs)	Organisations have flagged various recommendations /guidance points which may be problematic to implement/follow in practice. Numerous drafting changes have also been recommended (which we do not explain in detail).	• *Deadline*: One of the most common issues raised by organisations is the difficulty of implementing the new SCCs within a timeframe of one year. Many have argued that the implementation of the new SCCs is more than a repapering exercise – it would involve substantive discussions with contract parties and, once the parties agree on the terms and measures, flowing down the same to sub-processors would take time. For example, Workday argued that it has thousands of customer contracts that incorporate the SCCs, all of which must be amended to include the new clauses. Before that process can begin, the contracts with Workday's downstream processors should be amended to incorporate the new SCCs. Many organisations have asked the Commission to extend the timeframe – suggestions generally varied from two to five years. • *Replacement is not necessary*: Some organisations have also suggested that old (currently applicable) SCCs do not actually require replacing (until such time as the contract between the parties giving rise to the cross-border transfer is up for renewal), but they could be supplemented by additional measures as required by Schrems II. • *Costs*: Some organisations argued that only a few companies would be properly resourced to implement all of the proposed requirements and it would be unrealistic to expect all companies to have the resources to implement these requirements in practice. This would therefore create a competitive disadvantage, particularly for SMEs. • *Warranties*: The new SCCs require organisations to warrant conditions in third countries – at least one commenter (CIPL) argued that it is generally impossible "to warrant that an event will or will not occur when it has no direct control over it (such as a fire, flood, cyberattack or law enforcement request)". They suggested that the warranty obligation is replaced with an obligation to take measures appropriate to the risk (or it is tempered by an appropriate qualifier). • *Hierarchy*: The new SCCs state that, in case of conflict with another agreement, the new SCCs will prevail. Some organisations asked the Commission to clarify that, where the parties agreed on stricter terms, those terms will continue to apply (e.g. the new SCCs require controller importers to notify data breaches to exporters "without undue delay" but the parties may have agreed on a stricter timeframe (e.g. "immediately") or a relatively short timeframe (e.g. 24 hours)).

- *Privity of contract*: Some organisations argued that the new SCCs appear to create a relationship between the controller and the sub-processor by imposing direct obligations between them and this is not aligned with the GDPR or the general principles of contract law.
- *Further guidance*: Some organisations asked the Commission to publish guidance outlining different use cases and explaining how organisations are expected to comply with the new SCCs in respect of such use cases.
- *Drafting conflicts with GDPR*: Some organisations argued that some provisions of the new SCCs are not fully aligned with the GDPR provisions and suggested drafting changes accordingly (for example, many argued that the data breach notification test in the new SCCs does not track that of the GDPR).
- *Onward transfers*: Some organisations argued that the new SCCs adopt a more restrictive framework for onward transfers than allowed by the GDPR.

KEY SOURCES:

Core sources:

- Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems
- Charter of Fundamental Rights of the European Union
- Standard Contractual Clauses published by the European Commission (including the draft implementing decision)
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
- Recommendations 02/2020 on the European Essential Guarantees for surveillance measures
- Strategy for EU institutions to comply with"Schrems II" Ruling
- The CJEU's Advocate General (AG) issued a (non-binding) formal Opinion

Selected comments on the EDPB Recommendations:

- ICO statement on recommendations published by the European Data Protection Board following the Schrems II case
- White Paper in response to the Schrems II ruling (the US Department of Commerce, Department of Justice, & Office of the Director of National Intelligence)
- noyb
- US Chamber of Commerce
- ICANN
- European Banking Federation
- FEDMA
- Business Software Alliance (BSA)

Comments on Standard Contractual Clauses:

- Submissions to Standard Contractual Clauses
- EDPB & EDPS joint opinions on new sets of SCCs
- noyb
- The Centre for Information Policy Leadership (CIPL)
- Workday
- The Law Society of England and Wales and City of London Law Society

For further information, view our additional Privacy and Cybersecurity resources:

- Schrems II (Insight piece)
- Privacy and Cybersecurity Blog
- Dentons' Privacy Pod
- Europe Cookie Law Comparison Tool