Computer & Communications Industry Association
Tech Advocacy Since 1972

Ensuring Secure Data Transfers post '*Schrems II*'

The Court of Justice of the European Union's ("CJEU" or "the Court") judgement in case C-311/18 (the "*Schrems II*" decision) found that Standard Contractual Clauses ("SCCs") remain a valid legal mechanism for transferring data to non-adequate jurisdictions outside of the European Union.[1] However, the Court also recognised that additional steps may be necessary to ensure that SCCs afford an adequate level of protection depending on the circumstances of the transfers. This raises practical questions for any company transferring data to the 152 'non-adequate' jurisdictions, including some of the EU's most important trading partners, and they are looking to the European Data Protection Board and the European Commission for consistent answers.

Businesses within and beyond the digital sector rely on international transfers of data to engage with customers, securely process information, and contract with service providers. Secure and unencumbered data flows underpin the transatlantic and global economies, supporting multi-trillion euro international trade relationships.

In the years to come, the multiplication of adequacy decisions can provide the necessary certainty that businesses need to transfer data abroad. Until then, the Court envisions that exporters employing SCCs assess "all the circumstances" surrounding a data transfer to a 'non-adequate' jurisdiction, including, but not only, the existence and applicability of third country government data access legislation and practices. Such 'data transfer self-assessments' will necessarily involve complex analysis that is not customary for private organisations to conduct and may present a significant practical burden for businesses, especially for small and medium sized businesses.

Consistent guidance and enforcement will be critical for ensuring that organisations of all sizes have the information and clarity necessary to assess their legal bases for transfers and to transfer data securely. CCIA therefore welcomes the commitment of the European Data Protection Board (EDPB) and the European Commission to provide such guidance in the coming weeks.[2]

---

[1] Court of Justice of the European Union, Case C-311/18 "*Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*" (16 July 2020), at ¶ 149, http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN.

[2] Testimony of Didier Reynders & Dr. Andrea Jelinek before the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (3 September 2020), https://www.europarl.europa.eu/streaming/?event=20200903-1345-COMMITTEE-LIBE&start=2020-09-03T11:49:26Z&end=2020-09-03T13:55:15Z&language=en.

With this paper, CCIA invites the EDPB and the European Commission to consider the following clarifications in their forthcoming guidance:

1. As a rule of thumb, **recognise that the transfer of personal data to third countries which do not benefit from an adequacy decision remain valid**, providing that the level of protection of personal data transferred to a third country remains essentially equivalent to the General Data Protection Regulation;

2. Clarify the necessary steps and practices for companies to conduct a 'data transfer self-assessment'. Specifically:

    (A) **CCIA invites the European Commission, in coordination with the EDPB, to issue non-binding guidance on third-country laws and practices** which could give rise to disproportionate interference with EU citizens' data protection rights. This is an essential piece of information that companies need to obtain in order to decide if and how they should conduct their own transfer assessment;

    (B) **CCIA invites the EDPB to clarify the relevant factors to evaluate "all the circumstances"** surrounding a transfer of EU personal data;

    (C) **CCIA invites the EDPB to consider a non-exhaustive 'toolkit' of 'supplementary measures' including contractual, technical, and organisational safeguards** which data importers and/or exporters may consider implementing when a prior self-assessment concludes that the laws of the country of destination may disproportionately interfere with EU personal data in a given data transfer context.

3. Advise on **flexible documentation procedures** demonstrating individualised data transfer assessment.

We provide below several considerations which we hope the EDPB and the European Commission will find useful when preparing further guidance for data transfers to third countries which are not subject to an adequacy decision.

Our comments solely focus on data transfers performed under the legal grounds under General Data Protection Regulation ("GDPR") Article 46. As for other legal grounds such as those included in Article 49, we would welcome the EDPB to consider addressing the discrepancy between its existing guidance and the CJEU's findings about the scale of data transfers permitted under Article 49.[3]

[3] As a reminder, when the CJEU struck down EU-U.S. Privacy Shield, it argued in paragraph 202 that it is "appropriate" to do so since the derogations in Article 49 prevent "a legal vacuum" that would mitigate the "effects" of the invalidation of an adequacy decision. While the Court recognises that these derogations have their own conditions, it implies that individuals' consent or contract with a company or any other derogations is "appropriate" and therefore capable of replacing an adequacy decision that supports today's massive data flows between the EU and the U.S. or any other jurisdiction. This stands in stark contrast with existing EDPB guidelines 2/2018 (25 May 2018), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

1. Validity of data transfers to 'non-adequate' third countries

Consistent with the July FAQs of the EDPB,[4] CCIA believes that the **transfer of personal data to third countries which do not benefit from an adequacy decision remain valid, providing that the level of protection of personal data transferred to a third country remains essentially equivalent to the General Data Protection Regulation.**

In our view, the thrust of the CJEU decision is to ensure that transferred EU personal data is afforded a level of protection that is essentially equivalent to the General Data Protection Regulation, regardless of the mechanism used to transfer data.

CCIA cautions against statements which interpret the Court's decision as universally prohibiting data transfers to or advise organisations to switch to service providers within the EU or another country providing an appropriate level of protection.[5] The articulation of such blanket views threatens to undermine the development of consistent guidance and enforcement as well as organisations' ongoing efforts to comply with the Court's decision. Furthermore, reading a *de facto* data localisation mandate into the *Schrems II* decision would be inconsistent with the Court's judgement and impractical for companies participating in the modern digital economy.

CCIA recalls that the intent of Articles 46, 47, and 49 of the GDPR is precisely to enable data exporters and importers to compensate for the lack of an adequacy decision in a third country. In light of the CJEU decision, Standard Contractual Clauses (SCCs) and other legal grounds under Article 46[6] should remain valid mechanisms to transfer data to third countries which do not offer adequate protection through the substance and/or enforcement of its data protection laws). Similarly, the mere existence of disproportionate government access laws and/or the lack of sufficient remedies in a third country does not, on its own, prevent the transfer of EU personal data to that country under any legal grounds in Article 46, providing that the data importer and/or data exporter can mitigate the effects of such interference through supplementary measures.

---

[4] European Data Protection Board, "Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18" (23 July 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf.

[5] *See e.g.*, "Personal data may generally no longer be transmitted to the USA until the legal situation changes", statement from the Berlin Supervisory Authority (17 July 2020), https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf; "A data transfer to countries without an adequate level of data protection will therefore no longer be allowed in the future", statement from the Hamburg Supervisory Authority (16 July 2020), https://datenschutz-hamburg.de/pressemitteilungen/2020/07/2020-07-16-eugh-schrems; and see the lack of particularised review of "all the circumstances" surrounding (hypothetical) data transfers by Microsoft in the context of the performance of a service to the French Health Data Hub, as well as a general recommendation to use service providers which are only subject to EU laws, CNIL's observations submitted to the Conseil d'Etat (8 October 2020), https://assets.documentcloud.org/documents/7224049/Me-moireCnilHDH.pdf.

[6] The CJEU affirmed that "the level of protection [under Article 44] must therefore be guaranteed irrespective of the provision of [...] chapter [V] on the basis of which a transfer of personal data to a third country is carried out", CJEU at ¶ 92.

Consistent with the Court's findings, organisations relying on Article 46 mechanisms are expected to conduct a **self-assessment of "all the circumstances"** surrounding the transfer of data.[7] This assessment is a precondition to identify whether and, where relevant, which **supplementary measures** are needed and fulfill the requirements set out in the Court decision. Similarly, the CJEU explicitly **requires Supervisory Authorities to assess the lawfulness of a data transfer** under Standard Contractual Clauses **"in light of all the circumstances of that transfer."**[8]

The following comments develop specific considerations and suggestions for guidance that should inform both organisations conducting their data transfer self-assessments as well as Supervisory Authorities' oversight and enforcement.

2. Data transfer self-assessments: a three-step process

Any future EDPB guidance should make clear that companies' assessments of their personal data transfers under SCCs or other legal grounds under Article 46 differ from a Commission adequacy decision.[9] While Commission adequacy assessments are exclusively concerned with the protection afforded by a third country government, a private company can only evaluate the protections afforded in the context of transferring a specific dataset between a limited number of entities within a given jurisdiction.

CCIA therefore invites the EDPB and the European Commission to develop guidance envisioning data transfer self-assessments as a three-step process, and provide the necessary guidance on each of these steps:

- Determine the existence and application of laws that risk permitting disproportionate interference with EU personal data in the country of destination. For this, companies can only rely on guidance from the European Commission and the EDPB;

- Assess the risks of any identified laws, taking into account all relevant circumstances surrounding the data transfer;

- Where necessary, provide for supplementary measures to mitigate residual risks of disproportionate interference.

[7] *See* EDPB FAQs at 5.
[8] CJEU at ¶ 112, 121.
[9] CJEU at ¶ 104 and 105 refers to Article 45(2) as *one* of the "factors to be taken into consideration in the context of Article 46".

(A) Commission and EPDB guidance on the existence and application of third country laws

Identifying and evaluating the laws of third countries that may disproportionately interfere with EU data protection rights is a prerequisite to ensure compliance with the findings of the CJEU. However, such assessments require a depth of knowledge which most companies, including the largest and most resourceful, do not have. Companies are not, and will never be, in a position to identify and assess which laws in the country(ies) of destination, and limitations thereof, would fail to meet the EU's proportionality and necessity test. Furthermore, leaving this assessment to companies on an individual basis would inevitably lead to a fragmented implementation of the CJEU's judgment.

We believe that the **European Commission, in consultation with the EDPB, has a crucial role to play and should issue non-binding guidance on the existence and application of third-country laws and practices where data transfers under Article 46 merit further scrutiny**. The European Commission has the institutional credibility and the expertise in carrying out evaluations of third-country government data access laws, as is the case in the context of adequacy determinations.

This non-binding guidance should further inform enforcement carried out by Supervisory Authorities. As such, the **EDPB should be consulted throughout the Commission's evaluation process**, and have an opportunity to advise the Commission consistent with Article 70(1)(b) and (s) of the GDPR.

Actionable guidance on third country legislation may entail any relevant information that can help organisations determine whether their transfers need to be reviewed. This may include for instance information related to the categories of entities and / or services and / or nature of EU personal data captured by a foreign data access government legislation, as well as any relevant caveat, in law or in practice, that may apply.

To that effect, the European Commission is well positioned to engage with third country governments and seek any qualified input that may inform its own guidance. In doing so, the European Commission should encourage third-country governments to make additional relevant information public as to guide companies' subsequent data transfer self-assessment and Supervisory Authorities' enforcement.

CCIA acknowledges the herculean task of assessing the laws of 152 non-adequate jurisdictions, and we suggest first focusing at least on the EU's largest trading partners, including updated information from the United States, the UK,[10] China, India, Russia, Turkey, Mexico, Brazil, etc.[11]

[10] If the UK is not granted adequacy status by the end of the transition period (31 December 2020).
[11] Paul Verburgt, "Client and Supplier Countries of the EU27 in Merchandise Trade (value %)," European Commission, Directorate General for Trade (19 March 2020), https://trade.ec.europa.eu/doclib/docs/2006/september/tradoc_122530.pdf.

CCIA believes this guidance is a practical step that would significantly help companies throughout their self-assessment, including considerations for supplementary measures.

(B) Criteria relevant to assess "all the circumstances" of a data transfer

To help companies in their assessment, the CJEU points to the "non-exhaustive" list of circumstances in the country of destination (Article 45(2)) which companies should consider to determine the risks that their data transfers carry.[12] However, beyond the reference to Article 45(2), the CJEU remains silent on what other relevant "circumstances" companies should consider in their risk assessment.

We therefore invite the EDPB to **clarify "all the circumstances"** that companies should take into account when conducting an assessment of their data transfers, **and consider the effective application of any identified laws and the risk of interference that they carry**, including:

- Whether the scope of these laws is applicable to either **entities** involved in the transfer;
- Whether the **nature of the personal data** involved may be, in law or in practice, subject to a production order. While a data recipient may fall under the scope of foreign government access laws, the data it receives may be irrelevant to the execution of government data access requests;
- The **context and purpose of the transfer, including subsequent processing in the country of destination** (e.g. HR management, clinical trial, fraud prevention, employees' remote access to customer data for customer support services);[13]
- **Volume** of data potentially impacted relative to the overall volume of data transferred for the provision of the service;
- Whether any **existing legal, technical or organisational measures** implemented by the data importer and/or data exporter effectively prevent third-party access in the country of destination, including government access to data at rest and/or in transmission depending on the laws of the country of destination (e.g. anonymisation, tokenisation, data masking, encryption, decentralised transmission and/or storage, and other data minimisation measures);

The results of this assessment should aid parties in assessing what, if any, additional safeguards and clauses may be appropriate in order to ensure essentially equivalent protection of data transferred pursuant to SCCs and other mechanisms under Article 46.

(C) Supplementary measures

The CJEU's decision underscored that contractual terms between a data exporter and data importer may require the adoption of measures to supplement the guarantees offered by model clauses to ensure adequate protection of personal data in light of the law of the country of

[12] CJEU at ¶ 104.
[13] Partially informed by GDPR Recital 113 .

destination.[14] However, the court did not elaborate upon the nature and scope of these supplementary measures beyond noting that they may include "safeguards via contractual commitments" and "additional safeguards" to those offered by model clauses.[15]

Therefore, CCIA recommends that the EDPB develop a non-exhaustive "toolkit" of supplementary measures that may be appropriate to protect data transferred pursuant to SCCs. Such a "toolkit" should include guidance and considerations for the use of contractual and procedural mechanisms taking into account identified risks, costs, and the nature of the transfer. Potential supplementary measures include (a) technical safeguards, (b) procedures for responding to government requests, and (c) transparency reports.

i) Technical Safeguards

Parties to a transfer may contract to provide for the use of security features that protect data from unauthorised access and disclosure both in-transit outside of the EU and at-rest. Such protections may include end-to-end encryption, pseudonymisation, tokenisation, and other safeguards that would limit the ability for unauthorised actors to collect and/or decipher the data.

Further, organisations may implement data minimisation, retention, and erasure policies to ensure that data holdings are limited to what is necessary to accomplish the purpose of a transfer. Adherence to such policies will reduce the privacy impact of a subsequent unauthorised disclosure of information. Privacy and data security certifications may also help demonstrate the implementation of data minimisation and organisational security measures to limit or prevent data access.

ii) Procedures for Responding to Government Requests

As an additional supplementary measure, businesses may formalise processes and implement robust legal and operational policies for reviewing and responding to law enforcement data access requests. These procedures may include commitments to challenge requests that are not necessary and proportionate, and to produce the minimum amount of information required pursuant only to valid legal process. Where an identified third-country law provides no mechanism for compelling controllers and processors to produce personal data, an importer may contract that they will not provide voluntary assistance in the execution of that authority.

iii) Transparency Reports

Importers may commit to publishing transparency reports to the fullest extent permissible describing the types of government access requests they have received, the rates at which they have produced data in response to requests, and information on the number of affected individuals. A transparency report may further include a disclosure of whether the importer has

[14] CJEU at ¶ 133 & 134.
[15] CJEU at ¶ 134, GDPR Recital 109.

ever received a government data access order under an identified law. Such disclosures, alone or in combination with additional government reporting on the utilisation of identified laws, may allow exporters to assess that the identified laws do not pose a risk of unnecessary and disproportionate interference with the data subject to transfer.

3. Data transfer self-assessments: accountability & documentation procedures

Documentation will be an important practical step for data importers and exporters to undertake throughout their data transfer assessments and demonstrate compliance with the CJEU decision to the competent Supervisory Authority, either in the course of an ex ante consultation procedure or an ex post evaluation.

CCIA believes that **data exporters and data importers should be free to choose the most practical and suitable way to record the performance of a data transfer impact assessment,** the implementation of supplementary measures, and the division of responsibilities between the importer and the exporter throughout this process.

We caution against adopting guidance prescribing formalistic documentation procedures. Flexibility is important to allow each organisation to tailor their risk self-assessment to their particular situation, and adjust these assessments as circumstances surrounding the data transfers evolve (e.g. any relevant amendments to third country government data access laws).

For example, a data importer and a data exporter may choose to update their Data Protection Impact Assessments (DPIA) to take into account the specific data protection risks arising from the transfer, and the transfer alone. Additional contractual terms (aside from model clauses) may bind the parties to keep each other informed of any material or legal changes that would warrant a review of their DPIA and the consideration of supplementary contractual, technical organisational measures. But privacy and data security certifications may also help demonstrate the implementation of appropriate supplementary measures without requiring significant and overly detailed data transfer inventory.

*
* *

For further information, please contact:
Alexandre Roure, Senior Manager, Public Policy, CCIA Europe: aroure@ccianet.org
Keir Lamont, Policy Counsel, CCIA: klamont@ccianet.org