1 October 2021

Transfer Impact Assessments: Three Months In

Barbara Cosgrove
VP, Chief Privacy Officer, Workday

Maia Spilman
Sr. Legal Counsel Privacy, BCD Travel Services

Gretchen Ramos
Global Co-Chair Data, Privacy & Cybersecurity Practice, Greenberg Traurig
ramosg@gtlaw.com | 415.374.0216

Privacy+ Security Forum

Transfer Impact Assessments (TIA)

Privacy+ Security Forum

1. **Background - How We Got Here**
   a. GDPR Requirements
   b. 2020 Developments
      - *Schrems II*
      - *Draft* EDPB Recommendations
   c. 2021 Developments
      - *New Standard Contractual Clauses (SCC)*
      - *Final EDPB Recommendations*
2. **Transfer Impact Assessments**
   a. The Landscape
   b. Challenges

GDPR – Chapter V Requirements

Transfer of personal data to "third countries" outside EEA only permitted if *specific safeguards* apply.

- "**The easy way**" = Adequacy Decision of EU Commission (Art. 45)
  Requires "adequate level of protection" for personal data in third country
  E.g., re Argentina, Canada, Israel, Japan, New Zealand, Switzerland, Uruguay, Japan, United Kingdom
  Until July 2020: "EU-US Privacy Shield"

- **"The exceptional way"** = performance of contract, defense of legal claims, explicit consent, etc. (limited transfers) (Art. 49)

- "**The hard way**" = Authority's approval and extensive procedures required (Art. 46 & 47)
  (Approved) Binding Corporate Rules (BCR), (Approved) Code of Conduct, (Approved) Certification Mechanism

- "**The way out?" =** Standard Contractual Clauses (SCC) (Art. 46(2)
  Easy to implement mechanism for contractual obligations imposed on data importer
  "Old" SCC date back to pre-GDPR era; CJEU ruled that "supplementary safeguards" might be required

2020 Developments – Schrems II

- July 2020 - *Schrems II* judgment invalidated Privacy Shield & questioned validity of SCC absent supplementary measures.
  - *See* https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en

- CJEU specifically found:

> 133 It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection.

2020 Developments – Schrems II

CJEU also noted:

134 …… It is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses.

135 Where the controller or a processor established in the European Union is not able to take adequate additional measures to guarantee such protection, the controller or processor or, failing that, the competent supervisory authority, are required to suspend or end the transfer of personal data to the third country concerned. That is the case, in particular, where the law of that third country imposes on the recipient of personal data from the European Union obligations which are contrary to those clauses and are, therefore, capable of impinging on the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data.

EDPB Publications – Nov 2020

- November 2020 - European Data Protection Board (the "EDPB") published for public consultation:
  - **Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data**
    - *See* EDPB Guidance on Supplementary Transfer Measures and Surveillance Calls Into Question Future Use of SCCs for Data Transfers to US at https://www.gtlaw.com/en/insights/2020/11/edpb-guidance-supplementary-transfer-measures-surveillance-use-of-sccs-data-transfers-to-us
  - **Recommendations 02/2020 on the European Essential Guarantees for surveillance measures**

Fast Forward ⟶ June 2021

Privacy+ Security Forum

New EU Standard Contractual Clauses - Implementing Decision provides:

(19) The transfer and processing of personal data under standard contractual clauses should not take place if the laws and practices of the third country of destination prevent the data importer from complying with the clauses. In this context, laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679 should not be considered as being in conflict with the standard contractual clauses. The parties should warrant that, at the time of agreeing to the standard contractual clauses, they have no reason to believe that the laws and practices applicable to the data importer are not in line with these requirements.

See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN

Fast Forward ⟶ June 2021

(20) The parties should take account, in particular, of

- the **specific circumstances of the transfer** (such as the content and duration of the contract, the nature of the data to be transferred, the type of recipient, the purpose of the processing),
- **the laws and practices of the third country of destination** that are relevant in light of the circumstances of the transfer and
- **any safeguards put in place to supplement those under the standard contractual clauses** (including relevant contractual, technical and organisational measures applying to the transmission of personal data and its processing in the country of destination).

As regards the impact of such laws and practices on compliance with the standard contractual clauses, different elements may be considered as part of an overall assessment, including **reliable information on the application of the law in practice (such as case law and reports by independent oversight bodies), the existence or absence of requests in the same sector and, under strict conditions, the documented practical experience of the data exporter and/or data importer**.

Fast Forward ⟶ June 2021

Privacy+ Security Forum

EU Standard Contractual Clauses – Clause 14

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. …..

Fast Forward ⟶ June 2021

Privacy+ Security Forum

EU Standard Contractual Clauses – Clause 14

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

….

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

Fast Forward ⟶ June 2021

Privacy+ Security Forum

EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with EU level of protection of personal data, adopted 18 June 2021

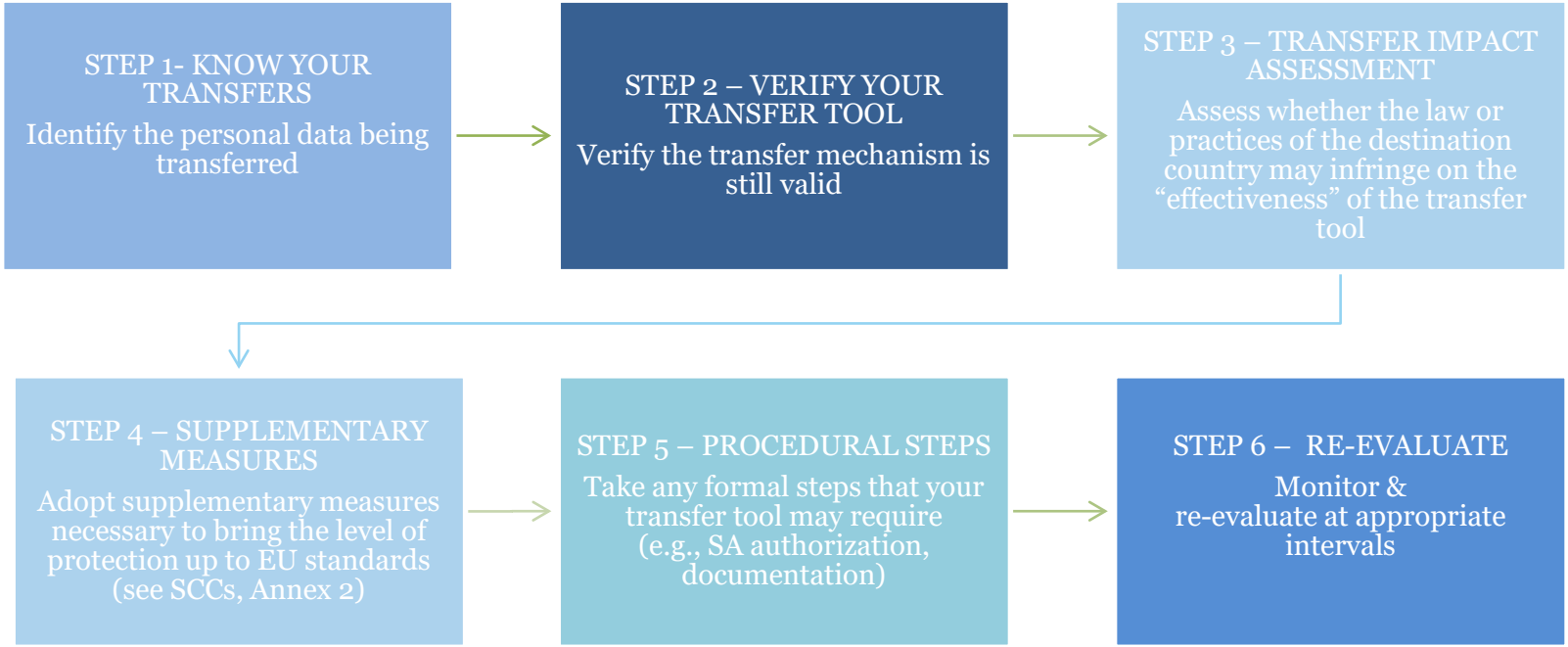
- Designed to help exporters with the complex task of assessing third countries and identifying appropriate supplementary measures where needed; and
- To provide exporters with a series of steps to follow, potential sources of information, and some examples of supplementary measures that could be put in place.

See edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (europa.eu)

Fast Forward ⟶ June 2021

Privacy+ Security Forum

EDPB Recommendations 01/2020 Six Step Process



EDPB Recommendations 01/2020 – Step Three, TIA

- EDPB notes organizations should conduct this assessment with due diligence and document it thoroughly as the competent supervisory and/or judicial authorities may request it and hold the organization accountable for any decision it takes based on the TIA.
- Organizations should assess if there is anything in the law and/or practices in force of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer.
- Focus first and foremost on third country legislation that is relevant to your transfer and the Article 46 GDPR transfer tool you are relying on.
    - When assessing the law of a third country dealing with access to data by public authorities for the purpose of surveillance, please refer to the EDPB European Essential Guarantees recommendations.
- Also examine practices of the third country's public authorities will allow you to verify if the safeguards contained in the transfer tool can ensure, in practice, the effective protection of the personal data transferred.

  This analysis especially relevant where:
  (i) legislation in the third country formally meeting EU standards is manifestly not applied/complied with in practice;
  (ii) there are practices incompatible with the commitments of the transfer tool where relevant legislation in the third country is lacking;
  (iii) your transferred data and/or importer fall or might fall within the scope of problematic legislation (i.e. impinging on the transfer tool's contractual guarantee of an essentially equivalent level of protection and not meeting EU standards on

TIAs in the Wild

Privacy+ Security Forum

Some examples of TIAs

- Twilio - https://support.twilio.com/hc/en-us/articles/4407117654555-Transfer-Impact-Assessment-Twilio-s-Onward-Data-Transfers
- Atlassian - https://www.atlassian.com/legal/data-transfer-impact-assessment
- Salesforce – Data Protection Impact Assessment https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Privacy/dpia-and-salesforce-services.pdf
- IAPP TIA Templates - https://iapp.org/resources/article/transfer-impact-assessment-templates/