

## – Whitepaper –

# Approach SD Worx to personal data transfers to third countries

## Introduction

This Whitepaper sets out the approach that SD Worx adopts towards transfers of personal data regulated by the GDPR to third countries (*i.e.*, countries outside the European Economic Area or “**EEA**”) that do not benefit from an adequacy decision in the context of the use of its products and services by its customers.

As for SD Worx, the Schrems II judgment (see below) has important implications for customers. With this Whitepaper, SD Worx aims to address concerns that customers might have regarding its data transfer approach and to support customers in managing the privacy risks associated with the transfer of personal data.

On 16 July 2020, the Court of Justice of the European Union (“**CJEU**”) issued its judgment in *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (Case C-311/18, hereinafter “**Schrems II**”). In Schrems II, the CJEU in essence:

- invalidated the EU-US Privacy Shield, in particular the Commission Decision 2016/1250 that constituted its legal basis;
- affirmed the general validity of the standard contractual clauses for data transfers, as published by the European Commission in its Commission Decision 2010/87/EU;<sup>1</sup> and
- proclaimed that organisations must verify, on a case-by-case basis, whether the law in the country of the importer/recipient affords a level of protection essentially equivalent to that guaranteed within the EU by the GDPR<sup>2</sup> to personal data transferred under such standard contractual clauses for data transfers.

These requirements have subsequently been subject to recommendations of the European Data Protection Board (the “**EDPB Recommendations**”).<sup>3</sup> In summary, these requirements anticipate that transfers to third countries using Standard Contractual Clauses (“**SCCs**”) (or other appropriate safeguards listed within Article 46 GDPR) will only be valid if the data exporter can verify, on a case-by-case basis, that the overall level of protection for personal data associated with the transfer, taking into account the specific circumstances of the transfer and any supplementary measures provided alongside the SCCs, does not undermine the level of protection guaranteed to data subjects under EU law and, in particular, the GDPR.

Following the Schrems II judgment and the EDPB recommendations, SD Worx has created a **data transfer impact assessment methodology** in cooperation with global law firm DLA Piper in order to ensure continuous compliance with the GDPR when transferring personal data from the EEA to third countries. The methodology provides required tools for SD Worx to assess safeguards when transferring personal data to third countries. It is fully aligned to the requirements of the GDPR following Schrems II.

---

<sup>1</sup> Later amended by Commission Decision 2016/2297.

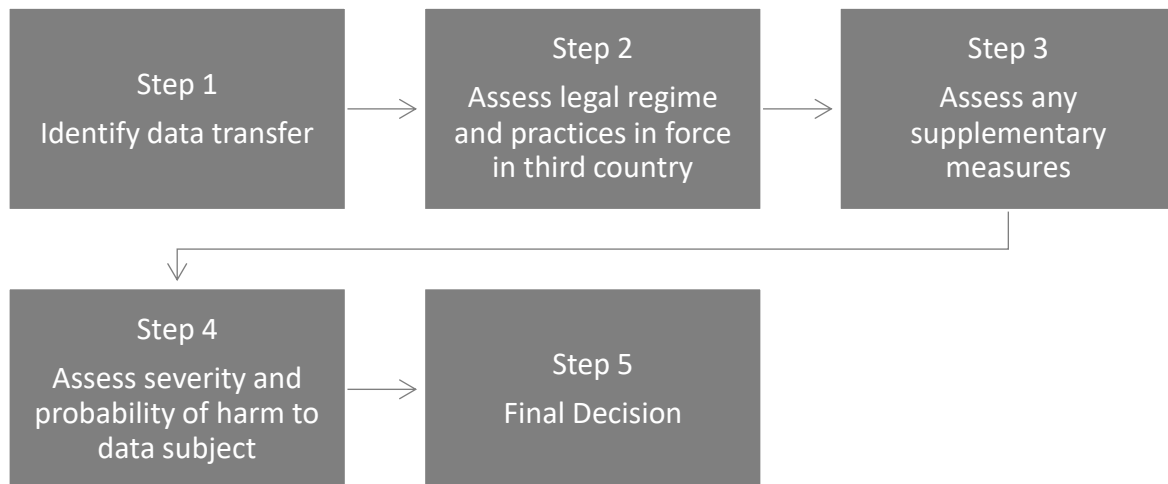
<sup>2</sup> Read in the light of the Charter of Fundamental Rights of the European Union.

<sup>3</sup> See Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, dated 18 June 2021 and issued by the European Data Protection Board on 21 June 2021.

## – Whitepaper – Approach SD Worx to personal data transfers to third countries

### Methodology

The methodology used by SD Worx includes a five-step assessment process, comprising an embedded scoring model to help manage decision making. It allows to logically and consistently assess, on a case-by-case basis, whether sufficient safeguards are in place to be able to proceed with the transfer.



#### Five-step assessment process

As a starting point, all SD Worx's legacy data transfers have been mapped and a process has been implemented to handle new transfers that could be initiated as our products and services evolve.

In a first step of the methodology, the specific circumstances of the transfer are assessed. This is a largely factual consideration of specific circumstances of the data flow associated with the transfer.

The second step assesses the extent to which the laws and practices in the destination country provide appropriate protection to data subjects (essentially equivalent guarantees), considering a number of factors such as the laws and practices authorising local public authorities to access or conduct surveillance on private information for national security or other reasons, individual redress options available to data subjects and the impact of relevant international treaties and related commitments.

In a third step, the relevant safeguards applied to the transfer are taken into account. Whereas the fourth step also factors in the severity of the potential residual risk of harm to which a data subject may be exposed following the transfer, and the likelihood of that harm arising in practice.

The last step involves a review of the risk score derived from the preceding steps to support a determination as to whether or not to proceed with the transfer.

#### Alignment with EDPB Recommendations

While the methodology has been designed to align with the CJEU's *Schrems II* decision and take account of the EDPB Recommendations, the six-step process of the EDPB has been intentionally re-structured as set out above. This relates mainly to:

## – Whitepaper –

### Approach SD Worx to personal data transfers to third countries

- The applicable transfer tools (Step 2 EDPB Recommendations), which are identified as part of step 1 of the methodology, whereas Step 3 of the EDPB Recommendations is included in steps 2-4 of the methodology;
- Step 4 of the methodology, which accommodates consideration of some risk-based factors into the assessment which will be carefully considered;
- Re-evaluation: The methodology is designed as an iterative process and its integration in the existing process flows of SD Worx automatically entails that the assessment will be re-evaluation at appropriate intervals (Step 6 of the EDPB Recommendations).

These nuances in application are intentional to provide a methodology that balances legally defensible decision-making with the practicalities of carrying out a risk-based impact assessment.

### Summary of the data transfer impact assessments

Below is a summary of the measures taken by SD Worx to implement this methodology. More specifically, the summary demonstrates the measures taken by SD Worx based on the five-step process to assess the transfers of customer personal data to third countries in connection with the provision of SD Worx’s services.

<p><b>Step 1:</b> <b>Identify data transfer</b></p>	<p>In relation to the processing of customer employee data (e.g. identification data, government identifiers, employment information, salary data) relating to the provision of payroll and HR services to customers, SD Worx entities located in the EEA/UK (data exporter(s)) engage their affiliates SD Worx (Mauritius) Limited, which is located in Mauritius and SD Worx d.o.o. Beograd, which is located in (Serbia) ( “Third countries”) .</p> <p>These data do not generally include special category data within the meaning of articles 9 or 10 GDPR, although in exceptional circumstances some health information may be processed when required for the applicable government declarations of the customer.</p> <p>The customer employee data are not stored in Third countries” and the access is limited to staff members in a role that requires access to the data to perform the relevant services.</p> <p>The transfers are based on module 3 (processor-to-processor) of the modernised 2021 standard contractual clauses (Commission Decision (EU) 2021/914)</p>
<p><b>Step 2:</b> <b>Assess legal regime and practices in force in third country</b></p>	<p>SD Worx, in cooperation with DLA Piper, has performed an assessment on the extent to which the legal framework in Third countries provides legal protections for personal data that are essentially equivalent to the guarantees offered within the EEA/UK. This part of the assessment involved consideration of five key criteria<sup>4</sup> regarding the legal framework and as a result an inherent risk score was established for each third country.</p> <p>Based on these assessments, SD Worx has identified the relevant areas of the third country legal frameworks that may impinge on the effectiveness of the appropriate safeguards provided by the standard contractual clauses. Therefore,</p>

---

<sup>4</sup> The five key criteria of the third country legal framework include an assessment on: regulation on the processing of personal data; regulation of public authority access to private data; regulatory supervision; rights of redress; and applicable international treaties.

## – Whitepaper –

### Approach SD Worx to personal data transfers to third countries

	SD Worx has reviewed its existing safeguards and has implemented new supplementary contractual and organizational measures.
<p><b>Step 3:</b> <b>Assess any supplementary measures</b></p>	<p>Taking into account the assessment in step 2, SD Worx confirms to have in place the following supplementary measures:</p> <ul style="list-style-type: none"> <li>• SD Worx’s payroll and HR services are certified under comprehensive industry standard security and privacy control frameworks;</li> <li>• SD Worx has adopted a pervasive set of security and privacy policies that govern SD Worx processing activities in relation to the payroll and HR services which are reviewed on an annual basis;</li> <li>• SD Worx has adopted a process dedicated to supervisory authority requests and which ensures that all relevant stakeholders are involved. SD Worx will adopt a more comprehensive policy which further expands the current government access request procedure with additional safeguards;</li> <li>• SD Worx adheres to a formal encryption policy which requires that any encryption of the customer’s personal data in transit is performed in accordance with accepted industry standards. Neither SD Worx Mauritius nor SD Worx Serbia store transferred personal data at rest in Mauritius or Serbia. All personal data transferred over public internet is encrypted in transit in accordance with accepted industry standards. Encryption key management is carried out with using industry best practices.</li> <li>• A well-developed access management procedure is in place to ensure access to personal data on a need-to-know basis with regular periodic controls by SD Worx.</li> <li>• Confidentiality obligations are imposed on all co-workers involved in the processing of the customer data.</li> <li>• SD Worx has put in place supplementary contractual safeguards with SD Worx Mauritius and SD Worx Serbia in order to reinforce and complement the safeguards that the SCCs provide.</li> </ul>
<p><b>Step 4:</b> <b>Assess severity and probability of harm to data subject</b></p>	<p>SD Worx has assessed the potential risk of harm to an individual arising from the transfers as well as the likelihood of that harm to occur. The assessments indicate that the risk of harm to an individual resulting from third country public authority access to customer personal data would be <b>low</b>. As some of the transferred data might be considered as confidential by the data subject, there might be some consequences for the data subject (e.g. distress). However, these data sets as such are generally not likely to generate severe consequences for the data subject.</p> <p>In addition, SD Worx assesses the likelihood of third country public authorities requesting access to any customer (personal) data as <b>low</b>. Although it cannot be excluded that the transferred personal data are of interest to third country public authorities, no such requests have been received by both SD Worx Mauritius and SD Worx Serbia so far. The transfers take place intra-group and no personal data are stored at rest as only remote access is possible from Mauritius or Serbia accordingly. In combination with the organisational measures analysed in the previous step, SD Worx assesses that the probability of harm arising in this context is <b>low</b>.</p>
<p><b>Step 5:</b></p>	<p>Based on the assessments carried out, SD Worx is confident that the implemented supplementary measures mitigate the risk of public authorities’</p>

## – Whitepaper –

### Approach SD Worx to personal data transfers to third countries

<b>Final Decision</b>	<p>access to customer’s personal data transferred to SD Worx Mauritius or SD Worx Serbia to an acceptable level.</p> <p>The standard contractual clauses used as a transfer mechanism do not need an authorization from a competent data protection supervisory authority and thus no additional formal procedural steps are necessary.</p> <p>SD Worx will conduct regular reviews of the data transfer impact assessment in order to ensure that any changes in the circumstances of the data transfers are taken into account.</p>
-----------------------	---

### Frequently asked questions (FAQ)

*SD Worx is aware that this remains a fast-evolving area of regulatory compliance with a range of emerging interpretations of the legal position by different data protection supervisory authorities within the EEA. Therefore, SD Worx reserves the right to amend the positions set out below at all times.*

*Q: When has SD Worx performed the data transfer impact assessments of the transfers taking place in the context of its products and services and have these assessments been updated since?*

We will seek to update the data transfer impact assessments of transfers as their features or other criteria within the assessment change and as regulatory guidance evolves.

The data transfer impact assessments for legacy transfers taking place to provide/perform its products and services will be reviewed on a regular basis, while new transfers will be subject to a review process before initiation of these transfers.

*Q: How does SD Worx deal with international transfers of personal data from the UK under the UK GDPR after Brexit?*

As the UK GDPR’s transfer regime still (largely) aligns with the EU GDPR, references to “EU” and “GDPR” in this Whitepaper can also be read as applying to the UK and the UK GDPR, as applicable.

The EDPB Recommendations are not applicable to personal data processed under the UK GDPR. We are awaiting guidance from the ICO on its approach to transfer impact assessments.

*Q: Does SD Worx rely on the new standard contractual clauses as published by the European Commission in its Commission Implementing Decision (EU) 2021/914 of 4 June 2021*

The transfers of personal data by the SD Worx EEA entities to SD Worx Mauritius and SD Worx Beograd in Serbia are the subject of an Intra-Group Agreement which incorporates modernised 2021 Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914), module 3 (processor-to-processor).

Moreover, we implemented UK Addendums to the SCCs for transfer of personal data by the SD Worx UK entity to SD Worx (Mauritius) Limited and to SD Worx Beograd in Serbia.

## **– Whitepaper – Approach SD Worx to personal data transfers to third countries**

The data transfer agreement will be updated with the relevant transfer clauses for processor-to-processor transfers when the competent authorities in the UK adopt new standard contractual clauses to replace the 2010 standard contractual clauses for transfers from the SD Worx UK entity.

### **Contact details**

Any questions concerning this Whitepaper or SD Worx's approach to international data transfers can be directed to:

[riskandsecurity@sdworx.com](mailto:riskandsecurity@sdworx.com)

This Whitepaper has been published on 28 December 2021 and has been last updated on 15 December 2025.