simmons+simmons

International data transfer compliance

2021

Globalisation of business requires the free flow of personal data across borders. However, data localisation/sovereignty features of various data protection laws present compliance challenges associated with international transfer of data.

In the EU and UK in particular companies face:

the requirement to conduct a data transfer risk assessment reviewing the law and practice in importing countries and determining the supplementary security measures required to match EU / UK standards of data protection

having to use the new EU standard contractual clauses (SCCs) for new transfers from September 2021 and replace the old EU standard contractual clauses with the new SCCs before December 2022 and, in due course, the UK SCCs

In order to help plan a compliance programme in relation to international data transfers we have set out below a suggested project plan.

1 Strategic advice and process creation

Undertaking a comprehensive review of international data transfers in a sophisticated company is a material undertaking and it requires a strategy for the conduct of the project and in relation to ongoing compliance. In this phase you should plan:

- how to approach the review of existing data transfers and making them compliant – for example, what is the company's risk appetite? Will a materiality threshold be applied to the transfers that will be reviewed and remediated?;
- how to operationalise the ongoing control and review of data transfers – what is the likely volume of ongoing compliance review required and what resources exist to enable the process to work effectively?; and
- the process for revalidation of transfer impact assessments and reviews of controls on an ongoing basis.

2 Data transfer mapping

Mapping of transfers can be a material exercise depending on the depth of the exercise that the company has determined it should undertake based on the strategy set in the first phase.
In order to ensure that the process is manageable we would advocate a functional review mapping out major transfers/systems/hosting environments/office locations. This review would ideally be conducted by reference to the different business units and identify the material:

- importing and exporting countries;
- applicable contract terms; and
- applicable technical and organisational controls.

The data transfer mapping exercise can draw on the Record of Processing Activities (RoPA) required to be in place by the GDPR as well as any prior work done in identifying data transfers/third parties with whom data is shared (e.g. as part of data processor contract remediation exercises).

3 Review of policies, procedures and other compliance documentation

This phase would include the review / creation of relevant policies, procedures and templates such as:

- content within general data protection policy;
- content within relevant privacy notices;
- data protection impact assessment template;
- data transfers policy / procedure;
- checklists for use in procurement processes / DDQs / third party risk assessment; and
- update to Record of Processing Activities based on the data transfer mapping exercise.

Thought needs to be given to how revised / new policies and procedures are communicated within the organisation and embedded in practices such as onboarding of new vendors.

4 Transfer impact assessments and identifying remediation measures

EU and UK laws (and the SCCs), in particular, require the conduct of data transfer impact assessments (TIAs) to assess whether there is adequate protection for the data in the importing country. This requires a review of the law and practice related to data protection and authority access to data / surveillance. In the event that there is a shortfall in protection "supplementary measures" must be implemented to further protect the data.

Conduct of TIAs therefore requires:

- review of law and practice in the importing country – this will establish how far short of equivalence the importing country is with the EU / UK and therefore the cap that must be closed / mitigated with supplementary measures;
- review of the facts of the data transfer (e.g. nature of the data / identity of the recipient / likelihood of authority access to data based on evidence of past activities)
- review of the controls in place in relation to the relevant data transfer (technical / operational / contractual); and
- identification of supplementary measures / remediation measures required.

Our CtrlTransfer tool enables the conduct of TIAs by providing the analysis of law and practice in 40+ countries.

5 SCCs repapering

The change to the EU SCCs and the forthcoming change to the SCCs to be used by UK companies will require a updates to SCCs in place with third party vendors and customers. It will also require execution of the relevant form of SCCs to cover intra-group transfers. To ensure ongoing ease of administration, we would recommend use of contract terms enabling more efficient amendment of the SCCs and entering into of SCCs with third parties going forwards by the appointment of group companies with authority to amend / enter into SCCs.

6 Other contractual documentation

Changes to the SCCs as well as the TIA requirements will require a review of procurement and customer contract templates such that they work effectively with the SCCs and enable the parties to meet their compliance responsibilities in relation to data transfers.

CtrlTransfer

Our data transfer solution

In an increasingly digitally connected world, we need an effective solution for completing international data transfer risk assessments. At Simmons & Simmons we have created a product to assist with this process, CtrlTransfer.

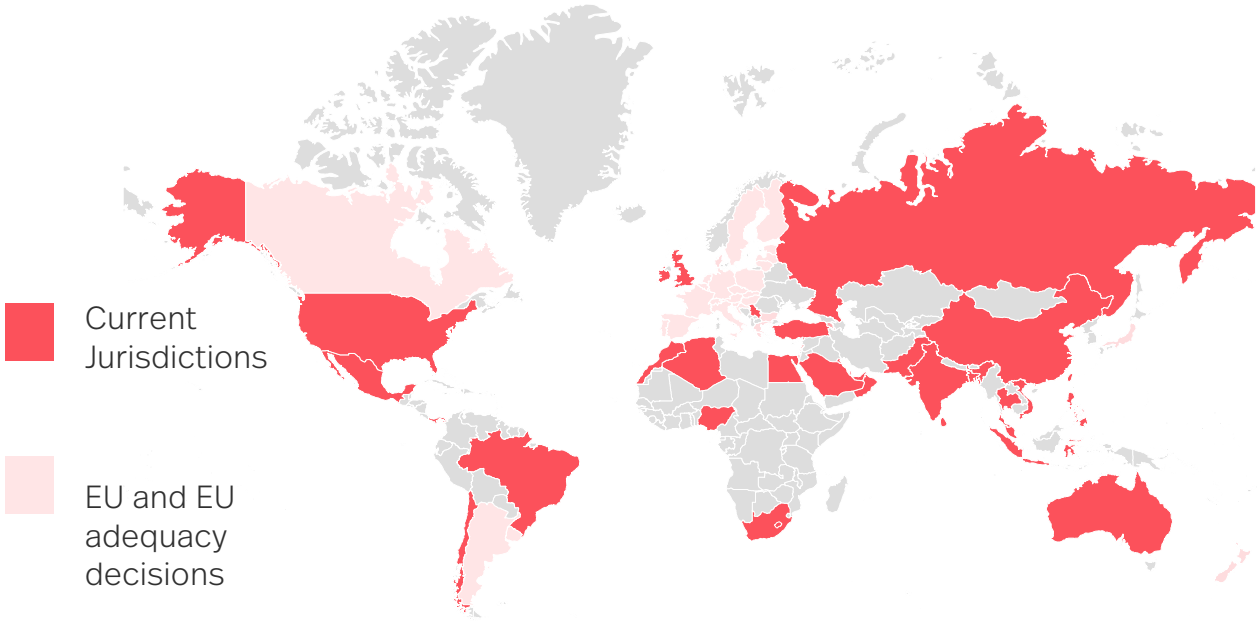
CtrlTransfer provides comprehensive analysis of over 40 jurisdictions supported by a simple scoring methodology, allowing for consistent and objective identification of key differences between the EU and non EEA jurisdictions.

Key product features include:

- A maintained database of comparative analysis of key non-EU jurisdiction's law and regulation related to privacy and surveillance against EU law and regulation
- Assessment templates and guidance
- An automated Standard Contractual Clause (SCC) generator
- Other data transfer toolkit items including standard contractual terms, and policy documents dealing with "supplementary measures"

Jurisdictions covered

Our database is customer led and covers the major jurisdictions likely to be recipients of data flows by European jurisdictions. Content is regularly updated to reflect any market/regulatory changes, ensuring it provides accurate current advice. Jurisdictions covered are highlighted below.



Key benefits

Efficiency
Cross jurisdictional information at your fingertips allows for quick analysis of data transfer.

Reliability
Regular updates to analysis with push notifications for subscribers provides confidence in the data provided.

Cost
The cost of the creation and maintenance of the database covering multiple jurisdictions is spread across all clients subscribing to the service. This results in a substantial cost saving.

Illustrative screenshots of CtrlTransfer

South Africa

§ Data Transfer Advice

3 **Overall**

Overall assessment: Laws related to data protection and surveillance, together with the Constitution, offer a reasonable degree of protection for individual rights, personal data and privacy. However, processing by a public body or government which involves national security and doesn't need to comply with the conditions for lawful processing of personal data.

3 **Guarantee A**
Processing sh
on clear, prec
accessible rul

3 **Guarant**
Necessity and
with regard to
objectives pur
be demonstra

3 **Guarant**
An independe
mechanism sl

3 **Guarant**
Effective reme
available to th

Comparative analysis of South Africa v EU

Please see below a table setting out a summary of the laws / regulatory environment applicable to the protection of personal data in South Africa and EU.[1]

	South Africa	EU
PART I: Data protection and privacy law (Relevant Guarantees: A & B)		
Is there law / regulation in place relating to the protection of personal data and privacy? Does the law lay down clear and precise rules governing the scope of these laws? If so, please summarise (at a high level) the main principles of that law and the	Yes, the POPIA,[1] which came into force on 1 July 2020 but provides for a one year grace period. The POPIA sets out a number of conditions for lawful processing of personal information[2] and applies to processing by automated means and non-automated	Yes, the GDPR[3]. The GDPR sets out seven key principles that apply to processing of personal data: (a) lawfulness, fairness and transparency; (b) purpose limitation; (c) data minimisation; (d) accuracy;

rity); and

scope of and type

a processing
d need to be
vidual.

the public or
rmation for a

Score explanation:
Guarantee D: Effective remedies need to be available to the individual

§

4 The guarantees offered by local law offer individuals effective and enforceable remedies to satisfy their rights when they consider that such rights have not been respected, including the ability to bring legal action. For example:
- There are effective remedies available to individuals through redress rights and notification, albeit in certain circumstances, notification might be delayed or avoided to avoid jeopardizing the purpose of the surveillance (e.g. individuals can bring legal action before an independent and impartial court)
- There is a data protection authority or other relevant authority that can take action on behalf of individuals

3 The guarantees offered by local law offer individuals reasonably effective and enforceable remedies, and individuals can bring legal action in most circumstances. For example:
- Data subjects can bring legal action in the courts and in most cases and have sufficient redress and notification rights
- There is a data protection authority or other relevant authority that can take action on behalf of individuals

2 The guarantees offered by local law offer individuals limited effective and enforceable rights. For example:
- Individuals can only bring legal action in the courts in limited circumstances and only have limited redress and notification rights
- It is difficult for individuals (or just EU citizens) to bring claims in the courts
- There is no data protection authority or other relevant authority that can take action on behalf of individuals

1 The guarantees offered by local law do not offer individuals effective and enforceable remedies. For example:
- Individuals cannot bring legal action before an independent and impartial court and / or cannot claim compensation where there is unlawful interference or unlawful processing of data
- There is no data protection authority or other relevant authority that can take action on behalf of individuals
- EU / UK citizens have no rights to bring claims or complain to a relevant authority

For additional information on our firm, please visit our website at **simmons-simmons.com**.