HUNTON

International Transfers

A Global Matter

What was once only a consideration in the context of cross-border transfers of personal data subject to the EU General Data Protection Regulation (GDPR) has now become a matter of global consideration. As businesses grow and new data protection laws are enacted globally, understanding international data transfer requirements is essential. The challenge for multinationals is navigating an increasingly complex landscape where global jurisdictions impose different rules and standards for international data transfers, complicating both operational efficiency and legal compliance. In many jurisdictions, data protection legislation restricts international transfers of personal data unless specific conditions are met. While complying with the myriad of requirements can initially seem daunting, there are methods businesses can leverage to streamline compliance and maximize operational efficiency.

At Hunton, we regularly advise our clients on compliance with cross-border data transfer requirements on a global scale. In this article, we will highlight the most common areas of overlap among data transfer requirements found in global data protection laws. Viewing international transfers requirements at a more holistic level, rather than per jurisdiction, eases the burden of complying with different legal regimes when transferring data within a corporate group. By identifying commonalities among different regulatory frameworks, businesses can seek to develop more efficient strategies for managing international data transfers.

Cross-Border Data Transfer Mechanisms

Since the introduction of the GDPR in 2018, we have seen a significant rise in the number of data protection laws enacted globally, most of which contain cross-border data transfer restrictions and conditions. Below is a summary of the key mechanisms available to multinationals that allow for or facilitate lawful cross-border transfers.

Adequacy Decisions

Adequacy decisions play a crucial role in the global landscape of data protection compliance and are generally the preferred mechanism for businesses to rely on when transferring data cross-border. An adequacy decision involves a local regulatory assessment of whether the laws of a third country provide an adequate level of protection for personal data, comparable to their own standards, or satisfy a similar test. When a third country is granted an adequacy decision, a business in the granting jurisdiction may transfer personal data to a business in the third country without implementing additional safeguards, such as those discussed below. At times, adequacy decisions are only made on a partial basis, i.e., they do not apply to all transfers of data to the third country. For example, transfers may only be permitted to businesses working in a specific sector of the third country. Obtaining adequacy status can be a detailed and rigorous process, and maintaining the status is based on continual scrutiny, including with respect to changes to the laws of the third country.

In the EU and UK, adequacy decisions are a critical component of the legal framework. In the EU, for example, the European Commission reviews various aspects of the third country's relevant legal framework, seeking to ensure it offers robust data protection principles, rights, and enforcement mechanisms. Where the European Commission finds that the data protection laws of a jurisdiction outside of the EU align with the requirements of the GDPR, they may elect to adopt an adequacy decision for that third country. Adequacy decisions in the EU are reviewed periodically, typically every four years, to ensure the relevant jurisdiction continues to provide adequate protection; an adequacy decision can be revoked or amended if standards are no longer being met to the satisfaction of the Commission.

The European Commission maintains a list of third countries which currently have adequacy decisions in place, and this list includes Andorra, Argentina, Brazil, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the UK, the US, and Uruguay. For certain of these jurisdictions, the European Commission has only agreed to partial adequacy. For example, the US has a partial adequacy decision which allows transfers of personal data to be made to organizations in the US which are eligible for, and adhere to, the EU-US Data Privacy Framework.

Similar to the EU and UK, several other jurisdictions utilize adequacy decisions as key components of their own legal frameworks, such as Argentina, the Abu Dhabi Global Market Free Zone (ADGM), Brazil, the Dubai International Financial Centre (DIFC), Japan, Nigeria, and Saudi Arabia.

Standard Contractual Clauses

Standard Contractual Clauses (SCCs), also known as "Model Clauses," are standardized contractual terms that businesses in certain jurisdictions can use as a mechanism for cross-border transfers of personal data. Jurisdictions that offer SCCs as a valid transfer mechanism include the EU, the UK, Brazil, China, the DIFC, Saudi Arabia, and China. SCCs generally outline the obligations of both parties to the contract (i.e., the data exporter and the data importer) and aim to set the standard of compliance by contract for the data importer at the level required by the data protection laws of data exporter's country.

Several forms of SCCs, such as those of the EU, the ADGM, and the Association of Southeast Asian Nations (ASEAN) Member States[1], utilize a modular approach, meaning they include multiple contractual modules that are tailored for different types of data transfers, such as controller-to-controller and controller-to-processor relationships. Other jurisdictions, such as Argentina, maintain a more traditional approach, with separate sets of SCCs for different types of transfers.

For most countries, implementing SCCs is usually a straightforward process: the SCCs only need to detail the relevant transfer taking place and be executed between the transferring parties either as a standalone agreement or through an appendix to an overarching agreement. Note, however, that the process required in China is slightly different. In China, a signed copy of the SCCs, along with a risk assessment related to the transfer, must be filed with the local provincial Cyberspace Administration in China for review and approval within 10 business days of executing the SCCs.

Binding Corporate Rules

Binding corporate rules (BCRs) are a third option available in select global jurisdictions to support cross-border data transfers. BCRs are internal policies adopted most commonly by multinational organizations to facilitate cross-border data transfers within the same corporate group. BCRs require approval from relevant data protection authorities and are legally binding once approved. BCRs aim to simplify compliance by reducing the need for multiple data transfer agreements between group entities, benefiting businesses with extensive international operations. The process of preparing and completing BCRs is both timely and costly, and for those reasons is a less commonly leveraged cross-border mechanism for most multinationals. For example, at present, approximately 200 BCRs have been approved in the EU despite the mechanism being available for over 15 years. Jurisdictions that recognise BCRs include the EU, the ADGM, Brazil, the DIFC, Nigeria, Singapore, and South Africa.

Transferor Obligations

Similar to both adequacy decisions and SCCs, certain jurisdictions allow personal data to be transferred internationally if the business transferring the data can ensure that the recipient in the third country will protect the personal data and/or the laws of the recipient jurisdiction provide a similar level of data protection to those of the transferring business jurisdiction. These requirements on the transferring business are most commonly addressed by leveraging contractual obligations with the recipient. In Australia, for example, the Australian Privacy Principles (APP) require the transferring business to take reasonable steps to ensure that the recipient of the data does not breach the APPs in relation to personal data, except where certain exceptions apply. Singapore takes a similar approach, requiring "comparable protection" for the transferred data as compared to the standards set out in the Singapore Personal Data Protection Act 2012. Other jurisdictions that follow a similar approach include Mexico, South Africa, and certain parts of Canada.

[1] Members of ASEAN include Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam.

Certifications

Another international data transfer mechanism recognized by certain jurisdictions is certifications. These certification schemes are typically established or approved by a jurisdiction at the local level, and businesses can then seek to rely on the scheme to lawfully transfer personal data outside that jurisdiction. A leading example is the Global Cross Border Privacy Rules (CBPR) System which provides an accountability-based certification for data controllers, with a parallel Global Privacy Recognition for Processors (Global PRP) System for processors. Certification is based on assessment against approved program requirements and is enforceable by relevant privacy enforcement authorities. While adherence to or participation in an available certification is not mandatory, it can be a useful tool for compliance with data transfer requirements.

China is an example of a country which employs certifications as a mechanism for cross-border data transfers. Effective January 2026, the Measures for the Certification of Cross-Border Personal Information Transfer issued by the Cyberspace Administration of China, allow a business to obtain a certification of personal information protection from a qualified professional institution, subject to satisfying certain conditions, e.g., the transfer involves personal data (excluding sensitive personal data) of more than 100,000 but fewer than 1 million individuals, or of sensitive personal data of fewer than 10,000 individuals. The certification is available to businesses inside and outside of China. Businesses outside of China can pursue certification either by designating an institution established by it in China or engaging a representative in China to facilitate the certification application.

Practical Tips for Compliance

Complying with several international data transfer requirements when transferring personal data intra-group, often simultaneously on account of data processing realities, requires a strategic approach. Below are steps that we recommend a business follow when seeking a practical approach to compliance for intra-group transfers at a global scale:

- **Map the data flows of the business:** The first step is to understand your data flows. This means identifying where personal data is collected, processed, stored, and transferred, within the business. This type of mapping exercise will help the company assess compliance needs and identifying potential risks.
- **Understand applicable laws:** Based on your understanding of the data flows, the next step is to identify those cross-border transfer requirements that apply to the business. This step involves understanding requirements of both the jurisdictions the business operates in and the locations outside of that jurisdiction where it transfers personal data. These first two steps are foundational to developing a strategic, comprehensive, and practical approach to compliance.
- **Implement an intra-group data transfer agreement:** Consider implementing an intra-group data transfer agreement that is flexible and adaptable to the business. An intra-group data transfer agreement can draw upon several of the mechanisms discussed above simultaneously, including memorializing between the group companies the reliance on adequacy decisions when they apply. Importantly, an effective intra-group data transfer agreement should allow for new group entities to accede to the agreement and for updates to be made to the agreement easily (and without written approval of all existing parties).
- **Other mechanisms:** Consider whether layering mechanisms could be useful, specifically certifications. Certain organizations, particularly very large global companies, opt to adhere to certifications even when they have other existing mechanisms in place, such as an intra-group data transfer agreement or BCRs. The adherence to certifications is a public commitment to compliant data transfers.
- **Stay informed and educated:** International data transfers are becoming subject to more regulation every year. Businesses must stay informed of changes to such requirements, consider how such requirements apply to their business, and, where relevant, adapt their practices accordingly.

Contact Us

At Hunton, we regularly assist clients with achieving their data processing goals while managing compliance with applicable cross-border transfer requirements, including developing holistic approaches similar to those summarized above. If you would like to discuss these requirements, and strategies to practically address them, please reach out to your Hunton privacy team partner contact:

Brittany Bacon
Partner, New York
bbacon@Hunton.com
+1 212 309 1361

David Dumont
Partner, Brussels
ddumont@Hunton.com
+32 2 643 58 18

Maeve Malik
Partner, New York
mmalik@Hunton.com
+1 212 309 1113

Aaron Simpson
Partner, New York
asimpson@Hunton.com
+1 212 309 1126

Adam Solomon
Partner, New York
asolomon@Hunton.com
+1 212 309 1327

Lisa Sotto
Partner, New York
lsotto@Hunton.com
+1 212 309 1223

Jonathan Wright
Partner, London
wrightj@Hunton.com
+44 (0) 20 7220 5620

HUNTON