International Data Transfers Toolkit

A Practical Guide for Fintech Companies

Prepared by Fintech Law

Based on 25+ years of cross-border regulatory experience across 33 jurisdictions

---

Introduction

International data transfers represent one of the most complex compliance challenges for fintech companies operating across multiple jurisdictions. This toolkit draws on Fintech Law's extensive experience advising major financial institutions including Morgan Stanley, American Express, Visa, and Citi Bank on cross-border data transfer compliance.

Having advised on data transfer frameworks across 33 jurisdictions, including complex implementations in the United States, Qatar, UK, and EU, we have developed practical approaches that balance regulatory compliance with business operational needs.

---

1. Understanding the Legal Framework

UK GDPR Requirements

The UK GDPR restricts transfers of personal data outside the UK unless specific safeguards are in place. Following Brexit, the UK operates its own adequacy regime separate from the EU.

Key Principle: Personal data can only be transferred internationally where:

- The destination country has an adequacy decision, or
- Appropriate safeguards are in place (such as Standard Contractual Clauses), or
- A specific derogation applies

EU GDPR Requirements

The EU GDPR applies similar restrictions but maintains its own list of adequate countries and its own version of Standard Contractual Clauses.

Practical Insight: In our experience advising Lloyds Banking Group and Credit Suisse International on EU-UK data flows post-Brexit, companies must now implement dual frameworks to ensure compliance with both regimes.

---

2. Adequacy Decisions

Current Adequacy Landscape (2025)

UK Adequacy Decisions include:

- European Economic Area countries
- Countries with EU adequacy decisions (by extension)
- Specific countries recognized under UK adequacy regulations

EU Adequacy Decisions include:

- Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, United Kingdom, Uruguay
- EU-US Data Privacy Framework participants

Case Example: When advising Toyota Financial Services on their global data processing operations, we implemented a tiered approach using adequacy decisions where available and SCCs for other jurisdictions, reducing compliance overhead by 40%.

---

3. Standard Contractual Clauses (SCCs)

EU Standard Contractual Clauses (2021)

The European Commission adopted new SCCs in June 2021, replacing the previous versions. These must be used for EU-origin data transfers.

Key Features:

- Four modules covering different transfer scenarios (controller-controller, controller-processor, processor-processor, processor-controller)
- Mandatory clauses that cannot be amended
- Optional clauses that can be customized
- Requirement for Transfer Impact Assessments

UK International Data Transfer Agreement (IDTA)

The UK ICO published its own International Data Transfer Agreement and an Addendum to EU SCCs for UK-origin data.

Practical Implementation: When implementing data transfer frameworks for Honda Finance Europe's operations across Asia-Pacific, we used the UK IDTA for UK-origin data

and EU SCCs for EU-origin data, with a unified governance framework to manage both.

---

4. Transfer Impact Assessments (TIAs)

Legal Requirement

Following the Schrems II decision, organizations must assess whether the laws and practices of the destination country provide adequate protection for personal data.

Practical Framework

Step 1: Identify the Transfer

- Map all international data flows
- Identify data categories and volumes
- Determine legal basis for processing

Step 2: Assess Destination Country Laws

- Review government access laws
- Assess surveillance frameworks
- Evaluate data protection enforcement

Step 3: Implement Supplementary Measures

- Technical measures (encryption, pseudonymization)
- Organizational measures (access controls, audit procedures)
- Contractual measures (additional safeguards)

Case Example: For a major cryptoasset exchange (confidential client), we conducted TIAs for data transfers to 15 jurisdictions, identifying specific risks in three jurisdictions and implementing end-to-end encryption and data minimization as supplementary measures.

---

5. Binding Corporate Rules (BCRs)

When to Consider BCRs

BCRs are appropriate for multinational organizations with frequent intra-group data transfers. They provide a comprehensive framework approved by data protection authorities.

Advantages:

- Single framework for all intra-group transfers
- Demonstrates strong compliance commitment
- Reduces need for individual SCCs

Disadvantages:

- Lengthy approval process (12-24 months)
- Significant implementation costs
- Ongoing compliance obligations

Practical Insight: In our experience advising Accenture on their global data governance framework, BCRs are most cost-effective for organizations with more than 500 regular international data transfers annually.

---

6. Derogations for Specific Situations

When Derogations Apply

Article 49 GDPR provides derogations allowing transfers without adequacy decisions or appropriate safeguards in specific circumstances:

- Explicit consent of the data subject
- Performance of a contract
- Important reasons of public interest
- Legal claims
- Vital interests protection

Critical Limitation: Derogations must be occasional and non-repetitive. They cannot be used as a systematic transfer mechanism.

Case Example: When advising British Gas on emergency data transfers during a cybersecurity incident, we relied on the vital interests derogation for immediate transfers, then implemented SCCs for ongoing data flows.

---

7. Sector-Specific Considerations

Financial Services

Additional Requirements:

- PRA and FCA expectations on outsourcing and third-country operations

- EBA Guidelines on outsourcing arrangements
- Operational resilience requirements

Practical Approach: For financial institutions, we recommend implementing a three-tier framework:

1. Adequacy decisions for routine transfers
2. SCCs with enhanced due diligence for critical service providers
3. Onshoring of critical functions where transfer risks are unacceptable

Payment Services

Specific Challenges:

- Real-time transaction processing requirements
- PSD2 strong customer authentication data flows
- Card scheme data localization requirements

Case Example: For CellPoint Digital's global payment processing platform, we designed a hybrid architecture with EU/UK data processing for European transactions and separate processing infrastructure for other regions, ensuring compliance while maintaining sub-second transaction times.

---

8. US-Specific Considerations

EU-US Data Privacy Framework

The EU-US Data Privacy Framework (DPF) provides an adequacy mechanism for transfers to participating US organizations.

Requirements for US Organizations:

- Self-certification to the Department of Commerce
- Annual re-certification
- Compliance with DPF Principles
- Submission to FTC or DOT enforcement

UK Extension: The UK has adopted its own extension to the EU-US DPF, allowing UK-US transfers under similar conditions.

Practical Insight: Having worked extensively in the United States, we advise clients that DPF certification is cost-effective for US organizations receiving significant volumes of EU/UK personal data, but SCCs remain necessary for onward transfers to non-DPF entities.

9. Practical Implementation Steps

Step 1: Data Mapping

Create a comprehensive inventory of all international data transfers:

- Source jurisdiction
- Destination jurisdiction
- Data categories
- Transfer volume and frequency
- Legal basis for processing
- Business purpose

Step 2: Gap Analysis

Assess current compliance status:

- Identify transfers lacking adequate safeguards
- Review existing SCCs for compliance with 2021 requirements
- Assess TIA requirements

Step 3: Implement Safeguards

Deploy appropriate transfer mechanisms:

- Execute new SCCs where required
- Conduct Transfer Impact Assessments
- Implement supplementary measures
- Update privacy notices

Step 4: Governance Framework

Establish ongoing compliance processes:

- Regular review of data transfer inventory
- Monitoring of destination country legal developments
- Vendor due diligence procedures
- Incident response procedures

Case Example: For Suzuki Financial Services' European operations, we implemented a quarterly data transfer review process that identified and remediated compliance gaps before they became regulatory issues, avoiding potential enforcement action.

---

10. Common Pitfalls and How to Avoid Them

Pitfall 1: Overlooking Onward Transfers

Issue: Many organizations focus on their direct transfers but overlook onward transfers by processors.

Solution: Contractually require processors to notify you of any onward transfers and ensure appropriate safeguards are in place.

Pitfall 2: Generic Transfer Impact Assessments

Issue: Using template TIAs without genuine assessment of destination country risks.

Solution: Conduct jurisdiction-specific assessments considering actual government access laws and practices.

Pitfall 3: Ignoring Technical Measures

Issue: Relying solely on contractual safeguards without implementing technical protections.

Solution: Implement encryption, pseudonymization, and access controls as supplementary measures.

Pitfall 4: Static Compliance Approach

Issue: Treating data transfer compliance as a one-time exercise.

Solution: Establish ongoing monitoring of legal developments and regular reviews of transfer mechanisms.

---

11. Regulatory Enforcement Trends

Recent Enforcement Actions

Data protection authorities across Europe have significantly increased enforcement of international transfer requirements:

- €746 million fine against Amazon (2021) - partly related to data transfers

- Multiple orders requiring suspension of transfers to US cloud providers
- Investigations into use of Google Analytics and Meta Pixel

Trend Analysis: Based on our monitoring of regulatory developments across 33 jurisdictions, we observe:

1. Increased scrutiny of transfers to the United States
2. Focus on adequacy of Transfer Impact Assessments
3. Expectations for robust supplementary measures
4. Sector-specific enforcement in financial services and healthcare

---

12. Future Developments

Areas to Monitor

UK-EU Adequacy: The EU's adequacy decision for the UK is subject to periodic review. Any changes could significantly impact UK-EU data flows.

US State Privacy Laws: Multiple US states have enacted comprehensive privacy laws with varying requirements for international transfers.

Digital Trade Agreements: International trade negotiations increasingly address cross-border data flows, potentially creating new transfer mechanisms.

Emerging Technologies: AI and machine learning create new data transfer challenges, particularly for training data and model deployment.

Conclusion

International data transfers require a sophisticated, multi-layered approach combining legal mechanisms, technical safeguards, and robust governance. Drawing on Fintech Law's experience implementing data transfer frameworks across 33 jurisdictions for major financial institutions, we recommend:

1. **Comprehensive data mapping** as the foundation
2. **Layered safeguards** combining adequacy, SCCs, and technical measures
3. **Genuine Transfer Impact Assessments** tailored to specific jurisdictions
4. **Ongoing monitoring** of legal and regulatory developments
5. **Business-aligned solutions** that enable operations while ensuring compliance

For specialist technical expertise on international data transfers, particularly for complex multi-jurisdictional fintech operations, contact Fintech Law.

About Fintech Law

Fintech Law provides specialist legal counsel on financial technology regulation, data protection, and cross-border compliance. With experience across 33 jurisdictions including the United States, Qatar, UK, and EU, we advise financial institutions, fintech companies, and large law firms on complex regulatory matters.

Contact: gavin.persaud@fintechlaw.uk