Cross-border data transfers: Conditions and exemptions

Table of contents:

IKIGAI LAW

Need for regulating cross-border data transfers

IKIGAI LAW

Rationale for regulating and safeguarding cross-border transfer of data:

- **Data Protection/Privacy** - To ensure that when citizens' data is transferred abroad, it is subject to similar protection as it would be within the country.
  - IT Act SPDI Rules, Clause 7, codifies this rationale.
  - EU - Adequacy Decisions
- **National Security -** Data essential for national security and public order may be intercepted or compromised when being transferred abroad.
- US has used its wide-ranging surveillance powers under the Patriot Act (now repealed), Section 702 FISA, and Executive Order 12333 to spy on foreign data subjects.
- China legal framework.
- **Law Enforcement -** To ensure law enforcement agencies can have access to data necessary for investigations, there are challenges in accessing it if stored abroad.
  - MLAT process is slow and often ineffective.
- **Trade**
- **Data Sovereignty.**
- **Economic Reasons**

Conditions for cross-border data transfers

IKIGAI LAW

- **Adequacy**
- **Consent**
- **Contracts**
- **Binding corporate rules**
- **Exceptions**
- **Certification**

Evolution of the Indian DPDP Act, 2023

IKIGAI LAW

- **Personal Data Protection Bill 2019**
  - Critical personal data - Cannot be processed outside India, except for two narrow grounds.
  - Sensitive personal data - Can be transferred abroad, but with the explicit consent of the data principal:
    - If approved by the DPA or the Central government.
    - A similar level of protection as under this bill is guaranteed.
    - This does not impact the liability of the data fiduciary and does not prejudicially affect the enforcement of relevant laws by Indian authorities.
  - Personal Data - No restriction.
- **Data Protection Bill, 2021 - Largely the same as but one key change:**
  - The central government can prohibit the transfer of sensitive personal data on the grounds of public policy or state policy.
- **Digital Personal Data Protection Bill 2022 –** Whitelist System – Cross-border transfer is only permitted to jurisdictions approved by the government.

Evolution of the Data Protection Law

IKIGAI LAW

- **Digital Personal Data Protection Act 2023 – Shift to a blacklist system**
  - Section 16 (1) The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified.
  - Section 16(2) Nothing contained in this section shall restrict the applicability of any law for the time being in force in India that provides for a higher degree of protection for or restriction on transfer of personal data by a Data Fiduciary outside India in relation to any personal data or Data Fiduciary or class thereof.
- **Other sectoral limits apply – rules issued by RBI, SEBI, DoT**

Comparative Practices – EU GDPR

IKIGAI LAW

- Article 44 - The transfer of personal data across EU's borders should not undermine the level of protection guaranteed by the GDPR.
- Article 45 - The EU Commission has the power to determine whether a country outside the EU offers an adequate level of data protection.
- The EU Commission has so far recognized 11 countries, including Andorra, Argentina, Israel, Japan, New Zealand, South Korea, Switzerland, UK, and US. The EU Commission reviews these adequacy decisions regularly.
- Art 42- Certification
- Art 46- Additional safeguards – SCCs, certification, BCR
- Art 47- BCR
- Art 49- derogations/exceptions

Case study: *Schrems I & II*

IKIGAI LAW

***Schrems I* (2015)**

- The Court examined whether the Safe Harbor arrangement governing data flow between the US and EU was consistent with the European Charter of Human Rights, and the Data Protection Directive.
- Held: Safe Harbor was not consistent with EU law as:
  - The framework was based on a system of self-certification for private companies, and there was no effective oversight system
  - Principles of Safe Harbour did not apply to US public authorities, and these authorities could disregard the safe harbour requirements when in conflict with the domestic laws.

***Schrems II* (2020)**

- After Schrems I, the European Commission approved the EU-U.S. Privacy Shield Framework.
- Held - Invalidated the EU-U.S. Privacy Shield Framework as:
  - U.S. surveillance programs permitted under the Privacy Shield, are not limited to what is strictly necessary and proportional
  - EU data subjects lack actionable judicial redress, they don't have a right to an effective remedy in the U.S.

Comparative Practices - EU

- **European Data Protection Board: - Standard after *Schrems I* and *Schrems II:***
  - The level and manner of protection do not have to be identical; rather, the adequacy test must require an ‘essentially equivalent’ level of protection.
  - Processing should be based on clear, precise, and accessible rules.
  - Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated.
  - An independent oversight mechanism should exist.
  - Effective remedies need to be available to the individual.

Comparative Practices – Singapore

IKIGAI LAW

- **Singapore Personal Data Protection Act 2012**
  - Any transfer of personal data abroad is to be in accordance with the requirements prescribed under the Personal Data Protection Regulations 2021, and the foreign countries should provide a comparable standard of protection to personal data (Section 26).
- **Personal Data Protection Regulations 2021 require:**
  - The individual to have given consent or is deemed to have consented.
  - Ensuring legally enforceable obligations against the recipient of personal data to provide transferred personal data a standard of protection comparable to that under the PDPA.
  - The personal data so transferred will not be used or disclosed by the recipient for any other purpose.
  - If the recipient organization holds a “specified certification” that is granted or recognized under the law of that country to which the personal data is transferred, the recipient organization is assumed to be bound by such legally enforceable obligations.
  - "Specified certification” refers to certifications under the Asia Pacific Economic Cooperation Cross Border Privacy Rules (“APEC CBPR”) System and the Asia Pacific Economic Cooperation Privacy Recognition for Processors (“APEC PRP”) System.

Comparative Practices – Cross-Border Data Transfer Mechanisms

IKIGAI LAW

- APEC Cross Border Privacy Rules (CBPR) Certification: The APEC CBPR System aims to bridge differing national privacy laws within the APEC region, reducing barriers to the flow of information. Organizations can be granted certification if they comply with the APEC Privacy Framework. Once certified, they can easily transfer personal data within the APEC countries.
- ASEAN Model Contractual Clauses: This model contract is based on the ASEAN Data Management Framework, aiming to ensure the transfer of data with trust and safety within ASEAN borders.
- Ibero-American Network for the Protection of Personal Data: This network permits the use of standard contractual clauses that comply with the Personal Data Protection Standards for Ibero-American States.

Contemporary Challenges

IKIGAI LAW

- Law enforcement agencies' access to data stored abroad: Agencies cannot undertake any enforcement action in other countries' jurisdictions. Thus, countries need to rely on cooperation with each other to access data abroad.
- Existing channels of cooperation like the Mutual Legal Assistance Treaty are considered slow and ineffective.
- US Cloud Act: It allows the US government to enter into executive agreements with foreign governments to allow foreign law enforcement agencies to access communications content directly from US service providers.
- The US entered into the first such agreement in October 2019 with the UK government; it signed an agreement with Australia in December 2011 and is in talks with the European Union as well.

Case study: CLOUD Act

IKIGAI LAW

- **Any agreement under the Cloud Act must:**
  - Afford 'robust' substantive protections for privacy and civil liberties.
  - Orders must only be passed to seek data related to a 'serious crime,' such as terrorism.
  - Orders should be specific, concerning a person, address, device, or similar identifier.
  - There must be a reasonable justification for issuing such orders, grounded in credible and articulable facts.
  - The orders should be subject to independent review or oversight.
- **Barrier to India signing an agreement with the US:**
  - Inadequate procedural safeguards indicated under Section 91 Cr.P.C.
  - Insufficient safeguards around interception and decryption.
  - Lack of accountability for intelligence agencies.
  - The DPDPA, while a welcome addition, fails to provide oversight and accountability for the interception powers of law enforcement.
  - Data localization mandates in the finance and telecom sector.

Thank you