Data Privacy Essentials for Cross-Border Businesses

Navigating the global patchwork of data protection regulations

LAWSEL ADVISORY

www.thelawsel.com

Table of Contents

CHAPTER 1

The Global Data Privacy Landscape

Over 140 countries now have data protection laws. For businesses operating across borders, navigating this patchwork is no longer optional — it is a commercial imperative that affects product design, vendor selection, and market entry strategy.

GDPR (European Union)

The General Data Protection Regulation remains the global benchmark. Key features:

- Applies to any organisation processing personal data of EU residents, regardless of where the organisation is based
- Requires a lawful basis for processing (consent, contract, legitimate interest, legal obligation, vital interest, public task)
- Mandates data protection by design and by default
- Grants extensive data subject rights (access, rectification, erasure, portability, objection)
- Requires Data Protection Impact Assessments for high-risk processing
- Imposes breach notification within 72 hours to the supervisory authority
- Fines up to €20 million or 4% of global annual turnover

GDPR enforcement has matured significantly. Regulators across EU member states issued over €4.4 billion in fines between 2018 and 2025.

DPDPA (India)

India's Digital Personal Data Protection Act 2023 is a significant development for businesses serving the Indian market:

- Applies to digital personal data processed within India and to processing outside India if it relates to offering goods or services to individuals in India
- Introduces the concept of 'Data Fiduciary' (controller) and 'Data Processor'
- Consent is the primary lawful basis, with 'certain legitimate uses' as alternatives
- Requires 'Significant Data Fiduciaries' to appoint a Data Protection Officer and conduct Data Protection Impact Assessments
- Establishes the Data Protection Board of India as enforcement authority
- Penalties up to ₹250 crore (approximately $30 million)
- Cross-border transfers permitted except to countries specifically restricted by the government

CCPA/CPRA (California)

The California Consumer Privacy Act, as amended by the California Privacy Rights Act, applies to businesses that:

- Have annual gross revenue exceeding $25 million, or
- Buy, sell, or share personal information of 100,000+ California residents, or

- Derive 50%+ of annual revenue from selling/sharing personal information

Key rights include the right to know, delete, correct, opt out of sale/sharing, and limit use of sensitive personal information. The California Privacy Protection Agency is the dedicated enforcement body.

Emerging Frameworks

Other jurisdictions with significant data protection frameworks include:

- Thailand (PDPA): Modelled on GDPR with some local variations. Fully effective since June 2022.
- China (PIPL): Strict data localisation requirements and consent-heavy framework. Cross-border transfers require security assessments for certain data volumes.
- UAE (PDPL): Federal data protection law effective January 2022. Includes DIFC and ADGM free zone frameworks.
- Saudi Arabia (PDPL): Effective September 2023 with a compliance grace period. Includes data localisation requirements.
- Singapore (PDPA): Balanced framework with a Do Not Call registry and mandatory breach notification.
- Brazil (LGPD): GDPR-influenced with 10 lawful bases for processing and an active enforcement authority (ANPD).

CHAPTER 2

Lawful Bases for Cross-Border Data Transfers

Transferring personal data across borders requires a legal mechanism. The available mechanisms vary by jurisdiction, and choosing the right one depends on the nature of the transfer, the data involved, and the relationship between the parties.

Adequacy Decisions (GDPR)

The European Commission can determine that a third country provides an 'adequate' level of data protection, enabling free data flows. Countries with adequacy decisions include Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, the United States (under the EU-US Data Privacy Framework), and Uruguay.

Adequacy decisions can be reviewed and revoked — as happened with the US Safe Harbor and Privacy Shield frameworks.

Standard Contractual Clauses (SCCs)

SCCs are the most widely used transfer mechanism. The current EU SCCs (adopted June 2021) cover four transfer scenarios:

- Module 1: Controller to controller
- Module 2: Controller to processor
- Module 3: Processor to processor
- Module 4: Processor to controller

Critical requirements when using SCCs:

- Conduct a Transfer Impact Assessment (TIA) for each transfer
- Assess whether the destination country's laws provide equivalent protection
- Implement supplementary measures if the TIA identifies gaps
- Document the assessment and keep it updated
- Include the SCCs in your contractual arrangements with the data importer

Binding Corporate Rules (BCRs)

BCRs are internal rules for multinational organisations that enable intra-group data transfers. They require approval from a lead supervisory authority and are suitable for:

- Large organisations with complex intra-group data flows
- Organisations that need a comprehensive, enterprise-wide transfer solution
- Situations where SCCs are impractical due to the volume and complexity of transfers

BCRs take 12–18 months to implement and approve. They are a significant investment but provide long-term flexibility.

Other Mechanisms

Additional transfer mechanisms include:

- Consent: The data subject explicitly consents to the transfer after being informed of the risks. Useful for one-off transfers but not scalable.
- Contractual necessity: The transfer is necessary to perform a contract with the data subject. Limited to direct contractual relationships.
- Codes of conduct and certification mechanisms: Emerging mechanisms under GDPR that are not yet widely adopted.
- Derogations: Available in limited circumstances (legal claims, vital interests, public interest). Not suitable for systematic transfers.

CHAPTER 3

Data Processing Agreements

When you engage a third party to process personal data on your behalf, a Data Processing Agreement (DPA) is legally required under GDPR, DPDPA, and most other data protection frameworks. A well-drafted DPA protects both parties and provides a framework for managing data protection obligations.

Essential DPA Provisions

Every DPA should address:

- Subject matter and duration of processing
- Nature and purpose of processing
- Types of personal data processed
- Categories of data subjects
- Obligations and rights of the controller
- Processor's obligation to process only on documented instructions
- Confidentiality obligations for personnel
- Security measures (technical and organisational)
- Sub-processing conditions and approval mechanisms
- Assistance with data subject rights requests
- Assistance with breach notification
- Audit rights
- Data return or deletion upon termination
- International transfer mechanisms (if applicable)

Sub-Processor Management

Managing sub-processors is one of the most operationally challenging aspects of data protection compliance:

- Maintain a current list of sub-processors (many organisations publish this on their website)
- Implement a notification mechanism for new sub-processors (typically 30 days' advance notice)
- Provide a meaningful objection right — the controller must be able to object to a new sub-processor
- Ensure flow-down obligations — sub-processors must be bound by equivalent data protection terms
- Conduct due diligence on sub-processor security and compliance

As a processor, your sub-processor management practices are a key differentiator. Enterprise customers will evaluate this during procurement.

Practical Tips

- Keep a template DPA that covers GDPR, DPDPA, and other applicable frameworks — do not negotiate from scratch each time
- Maintain a processing register that maps to your DPA obligations
- Automate sub-processor notifications where possible
- Include clear data deletion timelines — 'reasonable time' is not specific enough
- Address data residency and localisation requirements explicitly
- Include cooperation clauses for regulatory inquiries

CHAPTER 4

Data Subject Rights Across Jurisdictions

Data subject rights are the most visible aspect of data protection compliance. Failure to respond correctly and within required timelines is a common source of regulatory complaints.

Comparative Rights Overview

Right of Access:

- GDPR: Must respond within 1 month (extendable by 2 months)
- DPDPA: Must respond within 30 days (timeline may vary per rules)
- CCPA/CPRA: Must respond within 45 days (extendable by 45 days)

Right to Deletion/Erasure:

- GDPR: Right to erasure ('right to be forgotten') with specific exceptions
- DPDPA: Right to erasure of personal data
- CCPA/CPRA: Right to delete with specific exceptions

Right to Portability:

- GDPR: Right to receive data in structured, machine-readable format
- DPDPA: Not explicitly included
- CCPA/CPRA: Right to access in portable format

Right to Correction:

- GDPR: Right to rectification without undue delay
- DPDPA: Right to correction and completion
- CCPA/CPRA: Right to correct inaccurate personal information

Right to Object/Opt Out:

- GDPR: Right to object to processing based on legitimate interest or direct marketing
- DPDPA: Right to withdraw consent
- CCPA/CPRA: Right to opt out of sale/sharing; right to limit use of sensitive PI

Building a DSR Response Process

- [ ] Create intake channels (email, web form, in-product) that are easy to find
- [ ] Implement identity verification procedures — proportionate to the data sensitivity
- [ ] Log all requests with timestamps
- [ ] Route requests to the appropriate team based on type
- [ ] Track response deadlines by jurisdiction
- [ ] Develop template responses for each request type and jurisdiction
- [ ] Establish escalation procedures for complex requests
- [ ] Document all responses and reasoning
- [ ] Conduct periodic audits of DSR response quality and timeliness

CHAPTER 5

Building a Privacy Programme

A privacy programme is not just a set of documents — it is an operational capability that enables your business to process personal data lawfully, transparently, and securely.

Data Protection Impact Assessments (DPIAs)

DPIAs are required under GDPR when processing is 'likely to result in a high risk' to individuals. This includes:

- Systematic and extensive profiling with significant effects
- Large-scale processing of special category data
- Systematic monitoring of publicly accessible areas
- Use of new technologies where the impact is not yet understood

A DPIA should assess the necessity and proportionality of processing, identify risks to individuals, and document mitigation measures. Conduct DPIAs before processing begins — they are a planning tool, not a retrospective exercise.

Records of Processing Activities (ROPA)

Under GDPR, organisations must maintain records of processing activities. Your ROPA should include:

- Name and contact details of the controller/processor
- Purposes of processing
- Categories of data subjects and personal data
- Categories of recipients
- International transfers and transfer mechanisms
- Retention periods
- Technical and organisational security measures

Review and update your ROPA at least quarterly, and whenever you introduce new processing activities.

Privacy by Design

Privacy by design means embedding data protection into your product and business processes from the outset:

- Data minimisation: only collect what you need for the stated purpose
- Purpose limitation: do not repurpose data without a lawful basis
- Storage limitation: define and enforce retention periods
- Security: encrypt data at rest and in transit, implement access controls
- Transparency: clear, accessible privacy notices
- User control: give individuals meaningful choices about their data

Breach Response

Every organisation needs a breach response plan:

- Detection: How will you identify a breach? (monitoring, alerts, employee reporting)
- Containment: Immediate steps to limit the breach
- Assessment: What data was affected? How many individuals? What is the risk?
- Notification: GDPR requires notification to the supervisory authority within 72 hours. Notification to affected individuals is required when the breach is likely to result in a high risk.
- Documentation: Record all breaches, even those that do not require notification
- Remediation: Fix the root cause and update controls
- Review: Post-incident review to improve processes

CHAPTER 6

Practical Compliance Checklist

Multi-Jurisdiction Compliance Checklist

Use this checklist as a starting point for building your privacy compliance programme:

Legal Foundations:

- Identify all jurisdictions where you process personal data
- Map applicable data protection laws for each jurisdiction
- Determine your role in each processing activity (controller, processor, or joint controller)
- Identify lawful bases for each processing activity in each jurisdiction
- Review and update privacy notices for completeness and jurisdiction-specific requirements

Operational:

- Maintain a Records of Processing Activities (ROPA)
- Implement data subject rights response procedures
- Establish breach notification procedures and timelines for each jurisdiction
- Conduct DPIAs for high-risk processing
- Implement data retention schedules and deletion procedures

Contracts:

- Ensure DPAs are in place with all processors
- Implement appropriate cross-border transfer mechanisms
- Review vendor contracts for data protection compliance
- Include data protection provisions in employment contracts

Technical:

- Encrypt personal data at rest and in transit
- Implement access controls and authentication
- Enable audit logging for systems processing personal data
- Conduct regular security assessments
- Implement data loss prevention measures

Governance:

- Appoint a DPO where required (mandatory under GDPR for public bodies, large-scale systematic monitoring, and large-scale processing of special categories)
- Establish a privacy governance structure with clear accountability
- Deliver privacy awareness training to all staff
- Conduct periodic compliance audits
- Monitor regulatory developments in relevant jurisdictions

Ready to discuss your compliance needs?

Book a free 30-minute consultation to explore how LawSel Advisory can support your business.

BOOK A CONSULTATION

calendly.com/rini-thelawsel/30min

GET IN TOUCH

rini@thelawsel.com
www.thelawsel.com