Data Privacy Compliance Checklist

A Step-by-Step Guide to Building a Robust Privacy Programme

LAWSEL ADVISORY | WWW.THELAWSEL.COM

How to Use This Checklist

This checklist is designed for DPOs, General Counsel, and technology leaders at companies processing personal data across multiple jurisdictions. It covers GDPR, India's DPDPA, and CCPA/CPRA — adapt the scope based on where your users and operations are located. Items marked [PRIORITY] should be addressed first.

---

1. Regulatory Mapping & Scope

- [ ] **[PRIORITY] Identify which privacy regulations apply** based on where your users are located, where data is processed, and where your entity is established
- [ ] **Map your obligations under each applicable law**: GDPR (EU/EEA), DPDPA (India), CCPA/CPRA (California), POPIA (South Africa), PDPA (Singapore/Thailand), LGPD (Brazil), and others
- [ ] **Determine whether you are a controller, processor, or both** under each applicable framework — your obligations differ significantly
- [ ] **Identify sector-specific privacy requirements** (e.g., healthcare — HIPAA; financial services — GLBA; children's data — COPPA, Age Appropriate Design Code)
- [ ] **Document your regulatory mapping** and review it whenever you enter a new market or launch a new product

---

2. Data Inventory & Mapping

- [ ] **[PRIORITY] Create a comprehensive data inventory** — catalogue all personal data you collect, process, and store
- [ ] **Map data flows** end-to-end: collection points, processing activities, storage locations, sharing with third parties, and cross-border transfers
- [ ] **Classify data by sensitivity**: standard personal data, special category data (health, biometric, genetic, racial/ethnic origin), children's data, financial data
- [ ] **Identify all data processors and sub-processors** — maintain an up-to-date register with contractual status
- [ ] **Document retention periods** for each data category and implement automated deletion where possible

---

3. Legal Basis & Consent

- [ ] **[PRIORITY] Establish and document a lawful basis** for each processing activity (GDPR: consent, contract, legal obligation, vital interests, public task, legitimate interest)
- [ ] **For consent-based processing**: implement clear, specific, informed, and freely given consent mechanisms — pre-ticked boxes do not constitute valid consent under GDPR
- [ ] **Design consent flows that are granular** — allow users to consent to specific purposes separately rather than bundling
- [ ] **Implement consent withdrawal mechanisms** that are as easy as giving consent
- [ ] **For legitimate interest processing**: document your Legitimate Interest Assessment (LIA) including the balancing test
- [ ] **Under DPDPA**: ensure notice and consent requirements are met, with particular attention to processing children's data (verifiable parental consent required)

- [ ] **Under CCPA/CPRA**: implement "Do Not Sell or Share My Personal Information" mechanisms and honour Global Privacy Control signals

---

4. Privacy Notices & Transparency

- [ ] **Publish a comprehensive privacy notice** covering: identity and contact details of the controller, purposes and legal basis, categories of data, recipients, cross-border transfers, retention periods, and data subject rights
- [ ] **Ensure notices are written in clear, plain language** — avoid legal jargon; layer information where necessary (short notice + full policy)
- [ ] **Provide just-in-time notices** at the point of data collection (e.g., when a user submits a form, enables a feature, or shares data with a third party)
- [ ] **Maintain separate or supplementary notices** for employees, job applicants, and B2B contacts where applicable
- [ ] **Review and update notices** whenever processing activities, purposes, or recipients change

---

5. Cross-Border Data Transfers

- [ ] **[PRIORITY] Identify all cross-border personal data transfers** — including transfers to cloud providers, SaaS tools, and sub-processors in other jurisdictions
- [ ] **Determine adequacy status** of each destination country (EU adequacy decisions, UK adequacy regulations)
- [ ] **Implement appropriate transfer mechanisms** where no adequacy decision exists: Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or approved certification mechanisms
- [ ] **Conduct Transfer Impact Assessments (TIAs)** for transfers to countries without adequacy status — assess whether the destination country's legal framework provides adequate protection
- [ ] **Monitor regulatory developments** — adequacy decisions can be revoked (as with Schrems II invalidating Privacy Shield), requiring alternative mechanisms
- [ ] **Under DPDPA**: monitor the Data Protection Board's list of restricted jurisdictions for transfers of Indian personal data

---

6. Data Subject Rights

- [ ] **Implement mechanisms to respond to data subject requests** within statutory timeframes (GDPR: 1 month; CCPA: 45 days; DPDPA: as prescribed)
- [ ] **Support all applicable rights**: access, rectification, erasure, restriction of processing, data portability, objection, and rights related to automated decision-making
- [ ] **Verify identity** before fulfilling requests — implement a proportionate verification process
- [ ] **Train customer-facing teams** to recognise and escalate data subject requests
- [ ] **Log and track all requests** with response timestamps and outcomes for regulatory accountability

---

7. Data Processing Agreements

- [ ] **[PRIORITY] Execute Data Processing Agreements (DPAs)** with all processors — GDPR Article 28 mandates specific contractual terms
- [ ] **Ensure DPAs cover**: subject matter and duration, nature and purpose, data types, controller obligations, processor obligations (including sub-processor management, data breach notification, audit rights, and deletion/return on termination)
- [ ] **Review sub-processor chains** — processors must obtain controller authorisation before engaging sub-processors

- [ ] **Include AI-specific provisions** where processors use AI to process personal data: transparency about AI use, impact assessment obligations, human oversight requirements
- [ ] **Audit key processors** periodically — contractual rights are meaningless without exercise

8. Privacy by Design & Default

- [ ] **Embed privacy considerations into product development** from the design phase — not as a post-launch compliance exercise
- [ ] **Apply data minimisation** — only collect and process personal data that is necessary for the specified purpose
- [ ] **Implement privacy-protective defaults** — the most privacy-friendly settings should be the default (e.g., location tracking off by default, minimal data sharing)
- [ ] **Conduct Data Protection Impact Assessments (DPIAs)** for processing likely to result in high risk to individuals (mandatory under GDPR Article 35)
- [ ] **Integrate privacy checkpoints into your development lifecycle** — include privacy review in sprint planning, design reviews, and release processes

9. Data Breach Response

- [ ] **[PRIORITY] Develop and document a data breach response plan** covering detection, containment, assessment, notification, and remediation
- [ ] **Know your notification deadlines**: GDPR requires notification to the supervisory authority within 72 hours of becoming aware; DPDPA requires notification "without delay"
- [ ] **Define escalation criteria**: which incidents require regulatory notification, which require individual notification, and who makes the determination
- [ ] **Prepare template notifications** for regulators and affected individuals — you will not have time to draft these during an incident
- [ ] **Conduct tabletop exercises** at least annually to test response readiness
- [ ] **Maintain a breach register** documenting all incidents (including those not requiring notification) with facts, effects, and remedial actions

10. Vendor Privacy Management

- [ ] **Conduct privacy due diligence** before engaging any vendor that will process personal data on your behalf
- [ ] **Assess vendor privacy maturity**: certifications (ISO 27701, SOC 2), policies, breach history, sub-processor management, cross-border transfer practices
- [ ] **Maintain a vendor register** with privacy risk ratings, DPA status, and review dates
- [ ] **Monitor vendor compliance** on an ongoing basis — not just at onboarding
- [ ] **Plan for vendor exit** — ensure contracts provide for data return/deletion on termination

11. Employee Training & Awareness

- [ ] **Deliver privacy training to all staff** who handle personal data — at onboarding and periodically thereafter
- [ ] **Provide role-specific training** for high-risk functions: customer support, HR, marketing, product, and engineering
- [ ] **Train staff to recognise and report data breaches** — many incidents are first detected by front-line employees
- [ ] **Document all training** with dates, attendees, and content for regulatory accountability

12. Accountability & Documentation

- [ ] **Maintain Records of Processing Activities (ROPA)** as required under GDPR Article 30
- [ ] **Document all privacy decisions**: legal basis assessments, DPIA outcomes, consent mechanisms, transfer impact assessments
- [ ] **Appoint a Data Protection Officer (DPO)** if required (mandatory for public authorities, large-scale processing of special category data, or large-scale systematic monitoring)
- [ ] **Schedule periodic privacy programme reviews** — at minimum annually, and triggered by regulatory changes, new products, or market entry
- [ ] **Prepare for regulatory inquiries** — organise documentation so you can demonstrate compliance when asked

Quick Reference: Key Regulatory Thresholds

Regulation	Penalty Exposure	Notification Deadline	Key Deadline
GDPR	Up to 4% global turnover or EUR 20M	72 hours (to authority)	In force
DPDPA	Up to INR 250 crore (~USD 30M)	Without delay	Phased enforcement
CCPA/CPRA	USD 7,500 per intentional violation	N/A (AG enforcement)	In force

Next Steps

Privacy compliance is an ongoing programme, not a one-time project. The specific requirements for your organisation depend on your data processing activities, jurisdictions, and growth plans.

Lawsel Advisory designs and implements privacy programmes for technology companies scaling across jurisdictions — from regulatory mapping to operational playbooks.

Book a consultation: www.thelawsel.com **Email**: rini@thelawsel.com

This document is for informational purposes only and does not constitute legal advice. Regulatory requirements vary by jurisdiction and are subject to change.