Privacy Compliance Playbook

Workflows, templates, and checklists for data protection compliance

LAWSEL ADVISORY

www.thelawsel.com

Table of Contents

CHAPTER 1

Privacy Impact Assessment Workflow

When Is a PIA Required?

Conduct a PIA before starting any new processing activity that:

- Involves systematic and extensive profiling with significant effects on individuals
- Processes special category data (health, biometric, racial/ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, sexual orientation) at scale
- Systematically monitors publicly accessible areas
- Uses new technologies where the privacy impact is not yet understood
- Involves large-scale processing of personal data
- Matches or combines datasets from different sources
- Processes data concerning vulnerable individuals (children, employees, patients)
- Involves automated decision-making with legal or significant effects

Step-by-Step PIA Process

Step 1: Describe the Processing

- What personal data will be collected?
- From whom? (data subjects)
- For what purpose?
- How will it be processed and stored?
- Who will have access?
- How long will it be retained?
- Will it be shared with third parties?
- Will it be transferred internationally?

Step 2: Assess Necessity and Proportionality

- Is the processing necessary to achieve the stated purpose?
- Could the purpose be achieved with less data or less intrusive processing?
- Is the lawful basis appropriate and documented?
- Have data subjects been informed?

Step 3: Identify and Assess Risks

- What are the risks to individuals if data is lost, stolen, or misused?
- What are the risks of inaccurate or incomplete data?
- What are the risks of excessive data collection?
- What are the risks of unauthorized access or disclosure?
- Rate each risk: likelihood (low/medium/high) × impact (low/medium/high)

Step 4: Identify Mitigation Measures

- For each identified risk, document specific controls

- Technical measures (encryption, access controls, anonymisation)
- Organisational measures (policies, training, contracts)
- Assign responsibility and implementation timeline

Step 5: Sign Off and Review

- DPO review and approval (where applicable)
- Business owner sign-off
- Schedule periodic review (at least annually or when processing changes)
- Document the outcome and make it available for regulatory inspection

CHAPTER 2

Data Subject Request Procedures

Request Intake

- Maintain a dedicated email address for privacy requests (e.g., privacy@company.com)
- Provide a web form as an alternative intake channel
- Log every request immediately with: date received, requestor identity, request type, jurisdiction
- Send an acknowledgement within 2 business days
- Begin the response deadline clock from the date of receipt

Identity Verification

- Verify the requestor's identity before disclosing any personal data
- Proportionate verification — do not collect more data than necessary to verify identity
- For account holders: require login or verification from the registered email
- For non-account holders: request two forms of identification
- If identity cannot be verified, inform the requestor and explain what is needed
- Document the verification method used

Response Timelines

GDPR: 1 month from receipt (extendable by 2 months for complex requests — must notify within first month)
DPDPA: As prescribed by rules (expected ~30 days)
CCPA/CPRA: 45 days from receipt (extendable by 45 days with notice)
PDPA (Thailand): 30 days
PDPA (Singapore): 30 days
LGPD (Brazil): 15 days for simplified requests

- Set calendar reminders at 50% and 80% of the deadline
- If an extension is needed, notify the requestor before the initial deadline

Request Types and Actions

Access Request:

- Identify all systems containing the individual's personal data
- Compile data in a structured, commonly used format
- Include: categories of data, purposes, recipients, retention periods, source of data
- Provide a copy free of charge (first request)

Deletion/Erasure Request:

- Verify no legal obligation requires retention
- Check for other exemptions (freedom of expression, legal claims, public interest)

- Delete from production systems
- Queue deletion from backups (document backup retention timeline)
- Notify processors to delete
- Confirm deletion to the requestor

Correction Request:

- Verify the correct information with the requestor
- Update records in all systems
- Notify recipients who received the incorrect data
- Confirm correction to the requestor

Portability Request:

- Provide data in a structured, commonly used, machine-readable format (JSON, CSV)
- Limited to data provided by the individual and processed by automated means
- Transmit directly to another controller if technically feasible and requested

CHAPTER 3

Breach Notification Procedures

Breach Detection

- Implement automated alerting for unauthorized access attempts
- Monitor for data exfiltration indicators
- Establish employee reporting channels (internal hotline or email)
- Include breach detection in vendor monitoring
- Train all staff to recognise and report potential breaches immediately

Assessment and Classification

Within 24 hours of detection:

- Convene the incident response team
- Determine: what data was affected, how many individuals, what is the cause
- Classify severity:
  - High: sensitive data, large number of individuals, ongoing threat
  - Medium: personal data exposed, limited number of individuals, threat contained
  - Low: minimal data exposure, no sensitive data, no evidence of access
- Assess the risk to individuals (identity theft, financial loss, discrimination, reputational harm)
- Document all findings

Notification Requirements

Regulatory Notification:

- GDPR: Within 72 hours to the supervisory authority (unless unlikely to result in risk to individuals)
- DPDPA: Without unreasonable delay to the Data Protection Board
- CCPA: Without unreasonable delay to the Attorney General (if 500+ California residents affected)
- PDPA Singapore: Within 3 days to the PDPC (if significant harm or 500+ individuals)

Notification content (regulator):

- Nature of the breach and categories of data affected
- Approximate number of individuals affected
- Name and contact details of the DPO or contact point
- Likely consequences of the breach
- Measures taken or proposed to address the breach

Individual Notification (when high risk to individuals):

- Clear, plain language description of what happened
- What data was involved
- What you are doing about it
- What they can do to protect themselves

- Contact point for further information

Post-Breach Actions

- Conduct a root cause analysis
- Implement remediation measures
- Update security controls
- Review and update the incident response plan
- Deliver additional training if the breach resulted from human error
- Document lessons learned
- Brief leadership and the board

CHAPTER 4

Records of Processing Activities Template

ROPA Template Fields

For each processing activity, document:

- Processing activity name (e.g., 'Customer onboarding', 'Marketing email campaigns')
- Controller name and contact details
- Joint controller details (if applicable)
- DPO name and contact details
- Purpose of processing
- Lawful basis (and specific condition for special category data)
- Categories of data subjects (customers, employees, prospects, website visitors)
- Categories of personal data (name, email, IP address, payment data, etc.)
- Categories of recipients (internal teams, processors, third parties, regulators)
- International transfers (destination countries and transfer mechanism)
- Retention period or criteria for determining retention
- Technical and organisational security measures
- Date of last review
- Link to relevant DPIA (if applicable)

Maintenance Schedule

- Review the full ROPA quarterly
- Update immediately when new processing activities are introduced
- Update when existing processing activities change materially
- Update when processors or sub-processors change
- Update when retention periods are revised
- Assign a ROPA owner responsible for maintenance
- Make the ROPA available to the supervisory authority on request

CHAPTER 5

Vendor Privacy Assessment

Vendor Assessment Questionnaire

Before engaging any vendor that will process personal data, assess:

General:

- Where is the vendor incorporated and where does it process data?
- Does the vendor have a DPO or privacy lead?
- What certifications does the vendor hold (SOC 2, ISO 27001)?
- Has the vendor experienced any data breaches in the past 3 years?

Data Processing:

- What personal data will the vendor process?
- Where will the data be stored (geographic location)?
- Does the vendor use sub-processors? If so, who and where?
- How does the vendor handle data subject rights requests?
- What is the vendor's data retention and deletion policy?

Security:

- Does the vendor encrypt data at rest and in transit?
- What access controls are in place?
- How does the vendor handle security incidents?
- Does the vendor conduct regular penetration testing?
- What is the vendor's business continuity and disaster recovery capability?

Compliance:

- Is the vendor willing to sign your DPA?
- Does the vendor support the cross-border transfer mechanisms you require?
- Can the vendor provide evidence of compliance with applicable data protection laws?
- Does the vendor support audit rights?

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