DTE-I Privacy by Design Policy Template

Privacy by Design Implementation Policy

Document Information

- Version: 1.0
- Date: August 2025
- Author & Owner: Abed Al Rahman Naboulsi, CISSP / DTE-I Framework Initiative
- Validity: 12 months from policy approval date

1. PURPOSE AND SCOPE

This policy establishes requirements for implementing privacy-by-design principles in all technology systems that process personal information, ensuring compliance with privacy regulations while respecting individual dignity and autonomy.

Scope includes:

- All software development projects handling personal data
- System integrations involving third-party data sharing
- AI and machine learning systems processing individual information
- Cloud services and infrastructure hosting personal data
- Legacy system updates and modernization projects

2. ROLES AND RESPONSIBILITIES

- **Privacy Officer**: Overall policy compliance and privacy program governance
- **System Architects**: Technical privacy controls integration during design phase
- **Development Teams**: Code-level privacy implementation and testing
- **Product Managers**: Business requirement privacy impact assessment
- **Legal Team**: Regulatory compliance validation and risk assessment
- **AI Ethics Lead**: Algorithmic privacy and fairness considerations

3. CORE PRINCIPLES

3.1 Data Minimization

- Collect only data necessary for specified, legitimate purposes
- Implement technical controls preventing over-collection
- Regular reviews to identify opportunities for data reduction
- Default settings favor minimal data collection

Technical Implementation:

- Field-level validation preventing unnecessary data capture

- Purpose-specific data collection forms
- Automated data quality checks with minimization recommendations

3.2 Purpose Limitation

- Document specific purposes before data collection begins
- Technical enforcement of use limitations through access controls
- Regular audits ensuring data use alignment with stated purposes
- Clear consent mechanisms for purpose changes

Technical Implementation:

- Purpose-based access control lists (ACLs)
- Data tagging with purpose metadata
- Automated purpose compliance monitoring

3.3 Storage Limitation

- Default retention periods based on purpose and legal requirements
- Automated deletion workflows with exception approval processes
- Pseudonymization for extended analytical retention
- Regular retention policy reviews and updates

Technical Implementation:

- Automated data lifecycle management
- Retention schedule enforcement through database triggers
- Secure deletion verification procedures

4. TECHNICAL CONTROLS

4.1 Data Protection Impact Assessment (DPIA)

Mandatory triggers for DPIA:

- High-risk processing activities involving sensitive personal data
- Systematic monitoring of public areas or behavior
- Processing of special category data at scale
- AI systems making automated decisions affecting individuals

DPIA Process:

1. Initial risk screening using standardized questionnaire
2. Detailed assessment using DTE-I DPIA template
3. Risk mitigation planning with measurable outcomes
4. Stakeholder consultation (including data subjects where appropriate)
5. Regular reassessment based on system changes

4.2 Data Classification and Handling

Four-tier classification system:

- **Public**: Information intended for public disclosure
- **Internal**: Information for internal organizational use
- **Confidential**: Sensitive information requiring protection
- **Restricted**: Highly sensitive information with strict access controls

Handling Requirements:

- Automated labeling and policy enforcement where possible
- Encryption requirements based on classification level
- Access logging and monitoring for confidential/restricted data

- Regular classification review and accuracy validation

4.3 Access Controls

- Role-based access with principle of least privilege
- Regular access reviews and privilege right-sizing (quarterly minimum)
- Automated provisioning/deprovisioning based on HR systems
- Privileged access monitoring with real-time alerting
- Multi-factor authentication for all access to personal data

5. INDIVIDUAL RIGHTS ENABLEMENT

5.1 Rights Request Process

Supported Rights:

- Right of access (data portability)
- Right to rectification (correction)
- Right to erasure ("right to be forgotten")
- Right to restrict processing
- Right to object to processing
- Rights related to automated decision-making

Process Requirements:

- Single point of contact for all privacy rights requests
- Automated identity verification and request routing
- 30-day response standard with complexity-based extensions
- Quality assurance for request fulfillment accuracy
- Appeal mechanism for disputed responses

5.2 Consent Management

- Granular consent options with clear plain-language descriptions
- Easy withdrawal mechanisms with immediate technical effect
- Consent audit trails with timestamp and version tracking
- Regular consent refresh for ongoing processing activities
- Consent preferences synchronized across all touchpoints

6. MAQASID-INSPIRED VALUES INTEGRATION

Dignity Preservation (Hifz al-'Ird):

- Privacy controls that respect individual autonomy and personal boundaries
- Transparent communication about data practices
- Protection against reputational harm through secure data handling

Justice ('Adl):

- Fair and equitable treatment in all data processing activities
- Non-discriminatory data practices and algorithmic decision-making
- Equal access to privacy rights regardless of technical sophistication

Intellectual Integrity (Hifz al-'Aql):

- Clear, honest communication about data practices
- Educational resources to help individuals make informed privacy decisions
- Transparent AI systems that enhance rather than manipulate human understanding

7. MONITORING AND MEASUREMENT

Key Performance Indicators:

1. **Data Minimization Effectiveness**: % reduction in collected personal data fields year-over-year
2. **Rights Request Fulfillment**: % of requests completed within SLA (target: >95%)

3. **DPIA Completion Rate**: % of new high-risk systems with completed DPIAs (target: 100%)
4. **Privacy Training Completion**: % of relevant staff completing annual training (target: >98%)
5. **Privacy Incident Frequency**: Number of privacy incidents per quarter (target: minimize)
6. **Consent Withdrawal Response Time**: Average time to implement consent withdrawal (target: <24 hours)

Reporting Requirements:

- Monthly KPI dashboard for privacy team
- Quarterly report to executive leadership
- Annual privacy program assessment
- Incident-based reporting as required

8. GOVERNANCE AND REVIEW

Policy Governance:

- Quarterly policy effectiveness reviews by Privacy Officer
- Annual comprehensive policy updates incorporating regulatory changes
- Incident-driven immediate policy amendments when needed
- Stakeholder feedback integration through annual consultation process

Change Management:

- All policy changes require Privacy Officer approval
- Material changes require legal review and executive sign-off
- Communication plan for significant policy updates
- Training updates to reflect policy changes

9. COMPLIANCE AND AUDIT

Internal Audit Requirements:

- Annual privacy program audit by internal audit function
- Quarterly self-assessments using DTE-I checklist
- Continuous monitoring through automated compliance dashboards

External Validation:

- Third-party privacy assessments every two years
- Regulatory compliance reviews as required
- Industry benchmark participation for continuous improvement

APPROVAL AND SIGNATURES

Policy Owner: [Privacy Officer Name] _____ Date: _____

Legal Review: [Legal Team Lead] _____ Date: _____

Executive Sponsor: [Executive Sponsor] _____ Date: _____

Board Approval: [Board Chair/CEO] _____ Date: _____

Effective Date: [Date]

Next Review: [Date + 12 months]
