Privacy by Design
Framework for AI Systems

Type: Implementation Framework

Target Audience: Privacy Officers, AI Engineers, Data Protection Teams

This framework provides structured guidance for embedding privacy protections into AI systems from the earliest stages of design. Based on Privacy by Design principles adapted for AI-specific challenges.

1. Privacy by Design Principles for AI

Apply these seven foundational principles throughout the AI development lifecycle.

Principle	AI Application	Implementation
1. Proactive not Reactive	Anticipate privacy risks before building	Privacy impact assessment at design phase
2. Privacy as Default	Maximum privacy without user action	Minimal data collection; opt-in for more
3. Privacy Embedded	Privacy built into architecture	Technical controls, not just policies
4. Full Functionality	Privacy without sacrificing utility	Privacy-preserving ML techniques
5. End-to-End Security	Protect data throughout AI lifecycle	Training, inference, and storage security
6. Visibility and Transparency	Users understand data use in AI	Clear disclosure; explainable decisions
7. User-Centric	Individual control over personal data	Consent management; data rights

2. Data Collection Controls

Minimize data collection and ensure appropriate consent.

Data Minimization

□ Collect only data strictly necessary for the AI purpose
□ Document justification for each data element collected
□ Implement automated data expiration and deletion
□ Avoid collecting sensitive categories unless essential
□ Review data requirements at each development phase

Consent and Notice

□ Provide clear notice about AI processing of personal data
□ Obtain explicit consent for sensitive data use in AI

□ Explain how data will be used for training vs. inference
□ Disclose any third-party data sharing or model providers
□ Implement granular consent options where feasible

3. Privacy-Preserving Techniques

Technical methods to protect privacy while enabling AI functionality.

Technique	Description	Use Case	Implement?
Differential Privacy	Add noise to prevent individual identification	Model training, analytics	[ ] Y [ ] N
Federated Learning	Train on decentralized data without collection	Mobile apps, healthcare	[ ] Y [ ] N
Homomorphic Encryption	Compute on encrypted data	Sensitive inference tasks	[ ] Y [ ] N
Secure Enclaves	Isolated processing environments	Cloud AI processing	[ ] Y [ ] N
Data Anonymization	Remove or mask identifiers	Training data preparation	[ ] Y [ ] N
Synthetic Data	Generate artificial training data	When real data too sensitive	[ ] Y [ ] N

4. Data Subject Rights

Ensure AI systems support individual rights over personal data.

□ Right to Access: Users can obtain their data used in AI
□ Right to Rectification: Users can correct inaccurate data
□ Right to Erasure: Users can request data deletion
□ Right to Object: Users can opt out of AI processing
□ Right to Explanation: Users understand AI decisions affecting them
□ Right to Human Review: Users can request human intervention
□ Data Portability: Users can export their data

5. Training Data Governance

□ Document data sources and provenance
□ Verify lawful basis for using data in training
□ Assess and mitigate re-identification risks
□ Implement data retention limits for training sets
□ Test for memorization of personal data in models
□ Maintain audit trail of data processing activities

6. Third-Party AI Services

□ Review vendor data processing agreements
□ Verify vendor does not use customer data for training

□ Assess data residency and cross-border transfer
□ Ensure vendor security certifications (SOC 2, ISO 27001)
□ Document sub-processors and their data access

AI System: ________________________________

Privacy Officer: _________________________ **Date:** ______________