

Privacy by Design (PbD)

Enterprise Architecture Engineering Playbook

Architecture Review Board (ARB) Engineering Guidelines · Version 2.1

David Wright Sr – Enterprise Architect

Openthinka LLC

October 2026

Contents

1. Purpose of this Playbook	4
1.1 Why Enterprise Architecture owns the “How”	4
1.2 Scope	4
1.3 How to use this playbook	4
1.4 The value of applying PbD	5
2. The Privacy by Design Framework	6
2.1 What is Privacy by Design?	6
2.2 Mapping tasks to PbD requirements	7
2.3 Mapping controls to PbD requirements	7
2.4 Allocating responsibilities: the RACI	8
2.5 Regulatory mapping	9
2.6 Summary of the framework	11
3. The Seven Foundational Principles	12
3.1 Context	12
3.2 Proactive not Reactive; Preventative not Remedial	13
3.3 Privacy as the Default	13
3.4 Privacy Embedded into Design	14
3.5 Full Functionality: Positive-Sum, not Zero-Sum	14
3.6 End-to-End Security: Full Life Cycle Protection	15
3.7 Visibility and Transparency	15
3.8 Respect for User Privacy	15
3.9 Principles, strategies and NIST functions	16
4. The Personal Data Life Cycle	17
4.1 Acquisition and collection	17
4.2 Usage	17
4.3 Transfer or archival	17
4.4 Disposal	17
4.5 Controls by life cycle stage	17
5. PbD Across the Enterprise Architecture	19
5.1 Five steps toward a PbD-compliant E2E architecture	19
5.2 The privacy-aware layered view	20
5.3 Privacy touch points across the Customer Journey	21
5.4 Stakeholders and privacy accountability	22
5.5 PbD in M&A integration	23
6. Requirements Checklists	25
6.1 Enterprise privacy principles review	25
6.2 Pre-requirement checklist	25
6.3 Requirements for data protection and information security	25
6.4 Requirements for meeting data protection principles	26
6.5 Requirements to protect the rights of the data subject	27
6.6 Requirements to fulfil the organization’s obligations	27
6.7 Security of processing (C-I-A-R-T)	28
6.8 Acceptable level of risk	28
7. Architectural Checklist: the Eight Privacy Design Strategies	30
7.1 Strategy 1: Minimize	30
7.2 Strategy 2: Hide	30
7.3 Strategy 3: Separate	30
7.4 Strategy 4: Aggregate	30

7.5 Strategy 5: Control.....	31
7.6 Strategy 6: Inform.....	31
7.7 Strategy 7: Enforce	31
7.8 Strategy 8: Demonstrate	31
8. Design Checklist	32
8.1 Data-oriented design requirements	32
8.2 Process-oriented design requirements	33
8.3 Attack surface analysis and threat modelling.....	34
8.4 Why design requirements are necessary	35
9. Enterprise Privacy Capabilities.....	36
10. ARB Governance and Review Gates.....	37
10.1 Exceptions.....	37
10.2 Conclusion	38
Appendix A. NIST Privacy Framework Core Functions.....	39
A.1 IDENTIFY-P (ID-P).....	39
A.2 GOVERN-P (GV-P)	40
A.3 CONTROL-P (CT-P)	42
A.4 COMMUNICATE-P (CM-P)	43
A.5 PROTECT-P (PR-P).....	44
Appendix B. Regulation Cross-Reference	47
Appendix C. References	48

1. Purpose of this Playbook

This playbook gives Enterprise Architecture (EA), solution architects and engineering teams one repeatable method for designing and delivering systems that meet the principles and international standards of **Privacy by Design (PbD)**. It turns privacy requirements into architectural strategies, design checklists and review gates that the Architecture Review Board (ARB) can apply to any project, product, platform or acquisition.

Throughout, **the Enterprise** is the organization applying the playbook, the **Privacy Office** is the function led by the Chief Privacy Officer (CPO) that owns privacy policy and legal interpretation, and the **ARB** is the Enterprise Architecture Review Board that governs architectural decisions.

1.1 Why Enterprise Architecture owns the “How”

In most organizations the legal and business requirements for privacy, and their governance, are the responsibility of the Privacy Office. That group defines the **why** and the **what**. The engineering practice of **how**, particularly at the enterprise level, usually sits outside its brief. Solution-level tools may exist, but there is often no clear architectural guidance for privacy across systems, domains and journeys.

Enterprise solutions also include M&A integration and data migration, where privacy risk is concentrated:

- Data inherited in an acquisition may arrive with broken or unproven permissions (consent, purpose, lawful basis).
- Once merged with existing systems, inherited personal data that is not managed correctly can break permissions in the consolidated data set.

This playbook closes that gap. It defines best practice for managing personal information at the EA and solution-architecture level and gives the ARB criteria it can apply and audit.

1.2 Scope

- The architectural approach to the “how” of delivering enterprise solutions that embody the 7 Foundational Principles of PbD.
- A requirements framework that derives PbD requirements from the Fair Information Practices (FIPs) and maps them to tasks, roles and controls.
- Mapping of PbD requirements to major regulatory regimes (GDPR, LGPD, CCPA/CPRA, HIPAA) and to the NIST Privacy Framework.
- Checklists for pre-requirements, requirements, architecture and design, and the ARB review gates that use them.
- Application of PbD across the end-to-end (E2E) Customer Journey, the layered enterprise architecture and M&A integration.

The guidance is a reference framework. Teams can use it to derive more detailed criteria for application, audit and verification in their own context. It is not legal advice; the Privacy Office interprets the law for each case.

1.3 How to use this playbook

Part	Use it to	When
2. The PbD Framework	Derive PbD requirements, tasks and controls; map them to regulations	Strategy and requirements

Part	Use it to	When
3. The Seven Foundational Principles	Understand the principles and their engineering implications	Orientation and design reviews
4. The Personal Data Life Cycle	Locate controls at each stage of personal data handling	Requirements and design
5. PbD Across the Enterprise Architecture	Apply the 5-step E2E method, layered view and M&A pattern	Planning and due diligence
6. Requirements Checklists	Confirm the pre-requirements and requirements are complete	Requirements
7. Architectural Checklist	Apply the 8 privacy design strategies	Architecture
8. Design Checklist	Apply data- and process-oriented design requirements; threat model	Design and build
9. Enterprise Privacy Capabilities	Reuse shared privacy services instead of building point solutions	Architecture and build
10. ARB Governance and Review Gates	Pass the SLC privacy milestones with the right evidence	Throughout the life cycle
Appendices	NIST Privacy Framework Core; regulation cross-reference; references	Reference

1.4 The value of applying PbD

Value to the Enterprise

- Leadership in trusted, transparent management of personal information, demonstrated through innovative technology rather than policy statements alone.
- Automated, demonstrable compliance mechanisms designed for current regulation and adaptable to future regulation.
- A single, reusable set of systematic PII management capabilities available to every business system, product and service, and to customers and partners.

Value to customers

- Greater trust in the Enterprise as a supplier of products and services.
- The ability to manage personal data held or requested by the Enterprise and its partners in a quantifiable, objective way, whether or not a local regulator prescribes it.

Value to partners

- Greater trust in the Enterprise as a partner in the use of personal data the partner supplies.
- With Enterprise help, the ability to demonstrate automated compliance mechanisms of their own.
- Trust “reflected” from the partnership, and the ability to offer their customers the same level of PII management the Enterprise offers its direct customers by reusing Enterprise privacy services.

2. The Privacy by Design Framework

2.1 What is Privacy by Design?

Privacy by Design was conceived in the 1990s by Dr. Ann Cavoukian, then Information and Privacy Commissioner of Ontario, and adopted as an international standard by the International Assembly of Privacy Commissioners and Data Protection Authorities in 2010. It extends the eight Fair Information Practices (FIPs) developed by the Organization for Economic Co-operation and Development (OECD). In summary, PbD holds that the FIPs should be embedded as early as possible into the design of cloud and IT systems and data analytics models.

Embedding the FIPs first requires deriving generalizable, actionable **PbD requirements**. Those requirements are then met by organizational and technical measures, called **controls**. Each FIP translates into one or more PbD requirements.

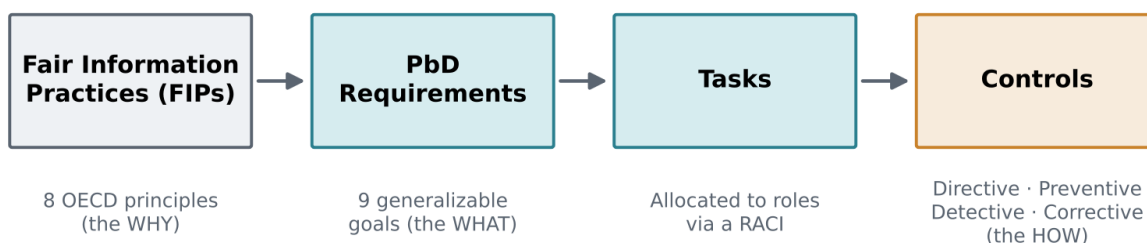


Figure 1: From Fair Information Practices to controls

Table 1: Deriving PbD requirements from the FIPs

Fair Information Practice	PbD requirements
1. Collection Limitation. There should be limits to the collection of personal data; any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.	Transparency; lawfulness and fairness
2. Data Quality. Personal data should be relevant to the purposes for which they are used and, to the extent necessary for those purposes, accurate, complete and kept up to date.	Data minimization; accuracy
3. Purpose Specification. The purposes of collection should be specified no later than at the time of collection, and subsequent use limited to those purposes or compatible ones specified on each change of purpose.	Purpose specification; purpose limitation
4. Use Limitation. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject or by the authority of law.	Purpose limitation
5. Security Safeguards. Personal data should be protected by reasonable security safeguards against loss, unauthorized access, destruction, use, modification or disclosure.	Security
6. Openness. There should be a general policy of openness about developments, practices and policies for personal data, including the existence and nature of the data, the main purposes of use, and the identity and usual residence of the data controller.	Transparency

Fair Information Practice	PbD requirements
7. Individual Participation. An individual should have the right to (a) confirm whether a controller holds data about them; (b) have it communicated within a reasonable time, at a reasonable charge, in a reasonable and intelligible form; (c) be given reasons if a request is denied and to challenge the denial; and (d) challenge data about them and, if successful, have it erased, rectified, completed or amended.	Intervenability
8. Accountability. A data controller should be accountable for complying with measures that give effect to the principles above.	Accountability

2.2 Mapping tasks to PbD requirements

PbD requirements can be rearranged into an organizational workflow so that tasks can be allocated between roles and areas of expertise.

Table 2: Mapping tasks to PbD requirements

PbD requirement	Task
Purpose specification	Express your purpose
Data minimization	Tailor the amount of data, number of data movements and duration of processing to the purpose
Accuracy	Ensure the accuracy of data
Lawfulness and fairness	Make sure processing means are lawful and fair
Purpose limitation	Preserve purpose over time
Security	Keep data and processing activities secure
Transparency	Keep processing activities transparent
Intervenability	Enable individuals to exercise their rights
Accountability	Take measures to demonstrate compliance with all prior principles

2.3 Mapping controls to PbD requirements

PbD requirements are **goals**. There is no single best way to meet them, so the right controls must be selected and implemented for each requirement and each context.

Table 3: Mapping controls to PbD requirements

PbD requirement	Task	Example controls
Purpose specification	Express purpose	1) Business owner expresses the purpose. 2) Privacy Office checks the legitimacy of the purpose.
Data minimization	Tailor data, movements and duration to purpose	1) Data user identifies the data relevant to the purpose. 2) Data policies (masking, differential privacy, etc.) ensure users access only what they need.
Accuracy	Ensure accuracy of data	1) A process to check accuracy. 2) Read-only access so data cannot be altered when consumed.
Lawfulness and fairness	Make sure processing is lawful and fair	A process to assess individuals' reasonable expectations for each use case.

PbD requirement	Task	Example controls
Purpose limitation	Preserve purpose over time	Purpose-based access control.
Security	Keep data and processing secure	1) Encrypt in transit and at rest. 2) Read-only access to underlying data where possible. 3) Regularly mask potential identifiers. 4) Strict access controls.
Transparency	Keep processing transparent	1) Transparent, documented pipelines. 2) Meaningful information for users.
Intervenability	Enable individuals to exercise rights	A self-service interface through which individuals submit and track requests.
Accountability	Demonstrate compliance	1) Fine-grained auditing and notification. 2) Regular, relevant reports on data activities.

Controls should be implemented from the design stage and combine different kinds of expertise. They are of four types:

Table 4: Control types

Control type	Purpose	Example
Directive	Specify tasks and expected behavior	Policy requiring a DPIA for any new processing of sensitive data
Preventive	Constrain behavior before it occurs	Purpose-based access control; default-off data sharing
Detective	Monitor to identify issues	Access-log anomaly detection; data discovery scans for untagged PII
Corrective	Mitigate issues once identified	Automated revocation and deletion workflows; breach response runbooks

These four types combine into two high-level categories: **process controls** (which role intervenes, when and how) and **system controls** (self-executing or automated decisions). Combining both is more effective than relying on either alone.

2.4 Allocating responsibilities: the RACI

Producing a RACI matrix (Responsible, Accountable, Consulted, Informed) before a processing activity starts allocates roles per task, and therefore per PbD requirement. The example below is for a data science project; it should be adapted for each initiative.

Table 5: Example high-level RACI for a data science project

PbD task	Business owner	Data user	Privacy / compliance	Data source admin	Cloud technology
Express purpose	A, R	C	C	I	
Tailor data, movements and duration to purpose	A	R	C	I	R
Ensure accuracy of data	A	C		R	R
Ensure processing is lawful and fair	A	R	C		R

PbD task	Business owner	Data user	Privacy / compliance	Data source admin	Cloud technology
Preserve purpose over time	A		R		R
Keep data and processing secure	A			R	R
Keep processing transparent	A	R	R		R
Enable individuals to exercise their rights	A		R		R
Demonstrate compliance with all prior principles	A	R	R		R

2.5 Regulatory mapping

PbD requirements form a common denominator across privacy regimes. The tables below show how each major regime expresses them. Section references are indicative; the Privacy Office confirms the applicable provisions for each case.

2.5.1 GDPR: Data Protection by Design (Article 25)

The EU General Data Protection Regulation (GDPR) obliges organizations processing personal data to perform **data protection by design (DPbD)**, a variant of PbD set out in Article 25. Article 25 requires appropriate technical and organizational measures, such as pseudonymization, designed to implement data protection principles such as data minimization effectively, and to integrate the necessary safeguards into processing to meet the Regulation's requirements and protect data subjects' rights.

Article 25 refers to the principles in Article 5, so DPbD requirements mirror PbD requirements:

Table 6: GDPR DPbD requirements

DPbD requirement	GDPR articles
Lawfulness, fairness and transparency	5, 6, 7, 12
Purpose limitation	5, 6
Data minimization	5
Accuracy	5
Storage limitation	5
Security	5, 32–34
Accountability	5, 24, 26, 28, 30, 35, 37–39
Intervenability	12–22

Because Article 25 draws in Article 5 and Articles 12–22, it acts as the backbone of the GDPR. Meeting Article 25 is the safest route to full GDPR compliance, which makes PbD central to any serious GDPR program.

2.5.2 LGPD: Brazil's General Data Protection Law

Brazil's Lei Geral de Proteção de Dados Pessoais (LGPD, Law No. 13,709/2018) is directly inspired by the GDPR. The similarities are much greater than the differences, although the LGPD's list of legal bases differs slightly and fairness is expressed partly through a principle of non-discrimination.

The **principle of prevention** in Article 6 of the LGPD requires measures to prevent harm arising from the processing of personal data. Implementing PbD controls as early as possible is fully aligned with it. The LGPD came into effect on 18 September 2020; its administrative sanctions, enforced by the national authority (ANPD), have applied since 1 August 2021.

2.5.3 CCPA as amended by the CPRA

The California Consumer Privacy Act of 2018 (CCPA) follows the GDPR less closely than the LGPD and contains no express by-design obligation. Even so, a PbD strategy makes CCPA compliance considerably easier, and many PbD requirements are explicitly addressed by it: purpose specification, purpose limitation, security, transparency, intervenability and accountability.

For example, purpose specification and limitation follow from the obligation to inform consumers of the purposes for which each category of personal information will be used, and from the prohibition on collecting additional categories, or using information for additional purposes, without notice.

The **California Privacy Rights Act (CPRA)** amendments, effective January 2023, strengthened this alignment. Section 1798.100(c) now requires that collection, use, retention and sharing be reasonably necessary and proportionate to the disclosed purposes, codifying data minimization and purpose limitation, and Section 1798.100(a)(3) requires disclosure of retention periods (storage limitation). Data minimization, previously only an implicit benefit, is now an explicit requirement. Accuracy remains good practice: keeping less data, and keeping it accurate, also reduces the volume of access, correction, opt-out and deletion requests.

Table 7: CCPA/CPRA PbD requirements

CCPA/CPRA PbD requirement	Sections (Cal. Civ. Code)
Purpose specification	1798.100; 1798.110; 1798.115
Data minimization	1798.100(c) (added by CPRA)
Accuracy	1798.106 right to correct (added by CPRA)
Lawfulness and fairness	1798.120; 1798.125
Purpose limitation	1798.100(a), (c)
Storage limitation	1798.100(a)(3) (added by CPRA)
Security	1798.100(e); 1798.150
Transparency	1798.100; 1798.130; 1798.135
Intervenability	1798.100; 1798.105; 1798.106; 1798.110; 1798.120; 1798.121; 1798.125; 1798.130
Accountability	1798.100(d); 1798.135; 1798.185 (risk assessments and cybersecurity audits, via regulation)

2.5.4 HIPAA

PbD requirements are consistent with older regulations too. The US Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects individually identifiable health information (protected health information, PHI). The Privacy Rule governs when covered entities may use or disclose PHI, lists the permitted purposes exhaustively, and requires the amount of data to be tailored to each purpose under the **minimum necessary** standard.

Table 8: HIPAA PbD requirements

HIPAA PbD requirement	Sections (45 CFR)
Purpose specification	164.502(a), (c); 164.506; 164.508; 164.510(b)(1); 164.512; 164.514
Data minimization	164.502(b); 164.514(d)
Accuracy	164.526
Lawfulness and fairness	164.506(b); 164.510
Purpose limitation	164.502(a), (c); 164.506; 164.508; 164.510(b)(1); 164.512; 164.514
Security	164.306; 164.308; 164.310; 164.312; 164.404–410; 164.502(h); 164.522(b); 164.514(a)(2)
Transparency	164.512(c)(2); 164.520
Intervenability	164.510; 164.522; 164.524; 164.526; 164.528
Accountability	164.314; 164.504; 164.508(a)(6); 164.514(b)(1)(ii); 164.514(d); 164.520(e); 164.530

A consolidated cross-reference of all four regimes is in Appendix B.

2.6 Summary of the framework

- Any serious effort to comply with multiple privacy laws, existing and future, should start by designing a PbD strategy and selecting controls that embed PbD requirements into processes, products and services as early as possible.
- Viewed correctly, PbD requirements are a common denominator for converging privacy regulation worldwide.
- Once they are met, differences between regimes, such as differing legal bases or conditions for exercising rights, become much easier to handle.
- Pursued as a strategy, privacy compliance becomes a competitive differentiator and a sign of organizational maturity; good governance translates into better market performance.

3. The Seven Foundational Principles

3.1 Context

With digital transformation, the value of information and the need to manage it responsibly have grown dramatically. Rapid innovation, global competition and increasing system complexity present profound challenges for informational privacy. Privacy has evolved beyond a legal compliance requirement into a market imperative and a critical enabler of trust.

Innovation increasingly follows a **design-thinking** approach: holistic, interdisciplinary, integrative and creative. Privacy must be approached the same way. It must be built into networked data systems by default, made integral to organizational priorities, project objectives, design processes and operations, and embedded into every standard, protocol and process that touches personal data.

The PbD framework rests on seven foundational principles that have been largely transposed into modern privacy legislation. They affirm the FIPs but go beyond them, raising the bar for privacy protection. They apply to technologies, business operations, physical architectures, networked infrastructure and entire information ecosystems.

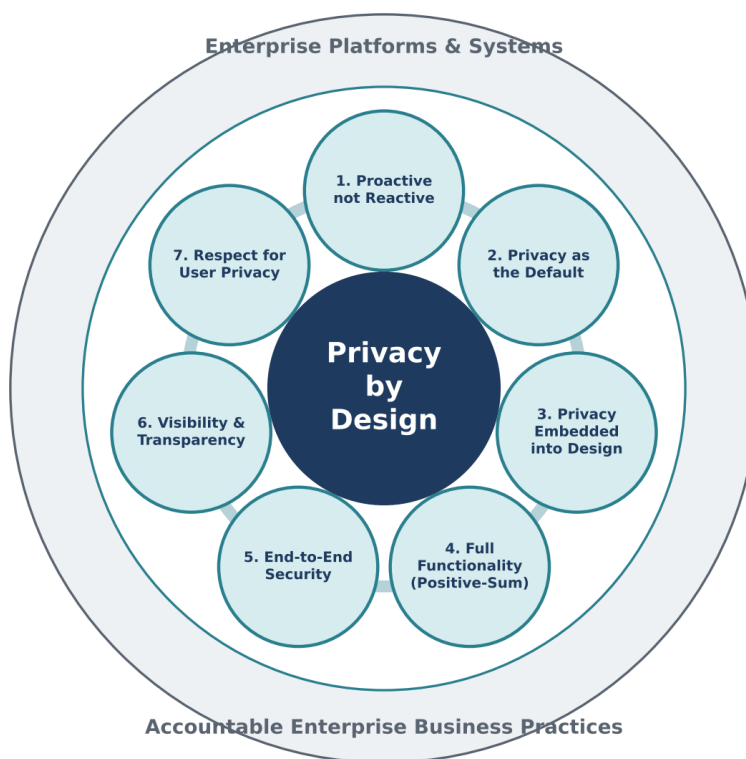


Figure 2: The seven foundational principles of Privacy by Design

Each principle below is followed by the FIPs that map onto it and, for this playbook, its **engineering implication**: what the ARB expects to see in an architecture.

3.2 Proactive not Reactive; Preventative not Remedial

PbD anticipates and prevents privacy-invasive events before they happen. It does not wait for privacy risks to materialize, nor offer remedies once infractions have occurred; it aims to prevent them. PbD comes before the fact, not after. It begins with an explicit recognition of the value of adopting strong privacy practices early and consistently, for example preventing internal data breaches from happening in the first place.

This implies:

- A clear commitment, at the highest levels, to set and enforce high standards of privacy, generally higher than those set by law and regulation.
- A privacy commitment demonstrably shared by user communities and stakeholders, in a culture of continuous improvement.
- Established methods to recognize poor privacy designs, anticipate poor practices and outcomes, and correct negative impacts well before they occur.

Engineering implication

Privacy requirements enter at the initiative requirements (IRD) gate, before concept approval. A data protection impact assessment (DPIA) and threat model exist before design is committed, and privacy risks are tracked in the project risk log like any other risk.

3.3 Privacy as the Default

PbD delivers the maximum degree of privacy by ensuring personal data are automatically protected in any IT system or business practice. If an individual does nothing, their privacy remains intact; no action is required of them, because protection is built in by default.

This principle, often called Privacy by Default, is informed by these FIPs:

- **Purpose specification:** the purposes for which personal information is collected, used, retained and disclosed are communicated to the data subject at or before collection, and are clear, limited and relevant.
- **Collection limitation:** collection is fair, lawful and limited to what is necessary for the specified purposes.
- **Data minimization:** collection of identifiable information is kept to a strict minimum. Designs begin with non-identifiable interactions and transactions as the default, and minimize identifiability, observability and linkability wherever possible.
- **Use, retention and disclosure limitation:** use, retention and disclosure are limited to the purposes identified and consented to, except where law requires otherwise. Personal information is retained only as long as necessary, then securely destroyed.
- Where the need for personal information is unclear, there is a presumption of privacy and the precautionary principle applies: default settings are the most privacy-protective.

Engineering implication

Every configurable setting ships in its most privacy-protective state. Optional data collection, sharing, tracking and profiling are off until the individual turns them on. Retention periods and automatic deletion are configured at build time, not left to operations.

3.4 Privacy Embedded into Design

Privacy is embedded into the design and architecture of IT systems and business practices, not bolted on after the fact. It becomes an essential component of the core functionality being delivered, integral to the system without diminishing functionality.

Embedding must be holistic (broader contexts are always considered), integrative (all stakeholders and interests are consulted) and creative (sometimes existing choices must be reinvented because the alternatives are unacceptable).

- Adopt a systematic, principled approach that relies on accepted standards and frameworks amenable to external review and audit, applying all FIPs with equal rigor at every step of design and operation.
- Wherever possible, carry out and publish detailed privacy impact and risk assessments that document the risks and the measures taken to mitigate them, including alternatives considered and metrics selected.
- Demonstrably minimize the privacy impact of the resulting technology, operation or information architecture, so it is not easily degraded through use, misconfiguration or error.

Engineering implication

Privacy capabilities (consent, data subject requests, classification, de-identification, retention) are consumed as shared Enterprise services (section 9) rather than re-implemented per application. Personal data is modeled explicitly in the Business Data Objects (BDOs), with classification and lineage as first-class attributes.

3.5 Full Functionality: Positive-Sum, not Zero-Sum

PbD accommodates all legitimate interests and objectives in a positive-sum, “win-win” manner rather than through a dated zero-sum approach of unnecessary trade-offs. It rejects false dichotomies such as privacy versus security, showing that it is possible, and far more desirable, to have both. PbD is doubly enabling: it permits full functionality and real, practical results for multiple parties.

- Embed privacy so that full functionality is not impaired and, as far as possible, all requirements are optimized.
- Reject positioning privacy as competing with other legitimate interests, design objectives and technical capabilities; accommodate them in an innovative, positive-sum way.
- Document all interests and objectives, articulate desired functions, agree and apply metrics, and reject trade-offs as often unnecessary in favor of solutions that enable multi-functionality.

Engineering implication

Architecture decisions that trade privacy for function must be recorded with the alternatives considered. The ARB challenges any zero-sum trade-off and asks whether techniques such as aggregation, pseudonymization, on-device processing or privacy-preserving analytics can deliver the function without the privacy cost.

3.6 End-to-End Security: Full Life Cycle Protection

Having been embedded before the first element of information is collected, PbD extends security throughout the entire life cycle of the data. All data are securely retained and then securely destroyed at the end of the process, in a timely fashion: cradle-to-grave, secure life cycle management, end to end.

There should be no gaps in protection or accountability. Without strong security, there can be no privacy.

- **Security:** entities assume responsibility for the security of personal information, commensurate with its sensitivity, throughout its life cycle, consistent with standards from recognized standards bodies.
- Applied security standards assure the confidentiality, integrity and availability of personal data throughout its life cycle, including secure destruction, appropriate encryption, and strong access control and logging.

Engineering implication

Every data store and flow carrying personal data in the E2E data-flow diagram shows its encryption, access control, logging and disposal mechanism. Backups, logs, analytics copies and test environments are in scope; production personal data is not used in development or test without de-identification.

3.7 Visibility and Transparency

PbD assures all stakeholders that, whatever the business practice or technology, it operates according to its stated promises and objectives, subject to independent verification. Its components and operations remain visible and transparent to users and providers alike: trust but verify. This principle tracks the FIPs in their entirety; for auditing, special emphasis falls on:

- **Accountability:** collecting personal information entails a duty of care. Responsibility for privacy policies and procedures is documented, communicated and assigned to a named individual. When personal information is transferred to third parties, equivalent protection is secured by contract or other means.
- **Openness:** information about policies and practices for managing personal information is readily available to individuals.
- **Compliance:** complaint and redress mechanisms are established and communicated, including how to reach the next level of appeal, and the necessary steps are taken to monitor, evaluate and verify compliance.

Engineering implication

The architecture produces evidence, not assertions: records of processing, data lineage, consent history and access logs that an auditor or data subject can inspect. Each processing activity has a named accountable owner recorded in the EA repository.

3.8 Respect for User Privacy

Above all, PbD requires architects and operators to keep the interests of the individual uppermost through strong privacy defaults, appropriate notice and empowering, user-friendly options. The best results are designed consciously around the interests and needs of individual users, who have the greatest vested

interest in their own data. Empowering data subjects to play an active role in managing their data may be the single most effective check against misuse. This principle is supported by:

- **Consent:** free and specific consent is required for collection, use or disclosure, except where law permits otherwise. The greater the sensitivity, the clearer and more specific the consent. Consent may be withdrawn later.
- **Accuracy:** personal information is as accurate, complete and up to date as necessary for the specified purposes.
- **Access:** individuals can access their information, learn its uses and disclosures, challenge its accuracy and completeness, and have it amended.
- **Compliance:** complaint and redress mechanisms are established and communicated to the public, including how to reach the next level of appeal.
- Beyond these FIPs, human-machine interfaces must be human-centered and user-friendly so informed privacy decisions can be exercised reliably. Business operations and physical architectures should show the same consideration, placing the individual at the center of operations that involve their data.

Engineering implication

Privacy controls are part of the user experience design, tested with users like any other feature. Consent, preference and rights requests are reachable in no more steps than the actions they govern, and their effect propagates to every downstream system.

3.9 Principles, strategies and NIST functions

The table links each principle to the architectural strategies of section 7 and the NIST Privacy Framework functions of Appendix A, giving reviewers a quick way to check coverage.

Table 9: Principle-to-strategy-to-NIST coverage map

Principle	Primary design strategies (section 7)	NIST Privacy Framework functions
1. Proactive not reactive	Enforce; Demonstrate	Identify-P; Govern-P
2. Privacy as the default	Minimize; Hide; Aggregate	Control-P
3. Privacy embedded into design	All eight strategies	Identify-P; Control-P; Protect-P
4. Full functionality	Aggregate; Separate; Hide	Control-P (disassociated processing)
5. End-to-end security	Hide; Separate; Enforce	Protect-P
6. Visibility and transparency	Inform; Demonstrate	Communicate-P; Govern-P
7. Respect for user privacy	Control; Inform	Control-P; Communicate-P

4. The Personal Data Life Cycle

Managing personal data is a data management problem, so it must be considered across the end-to-end life cycle. Four stages apply to every item of personal data, whatever the system.

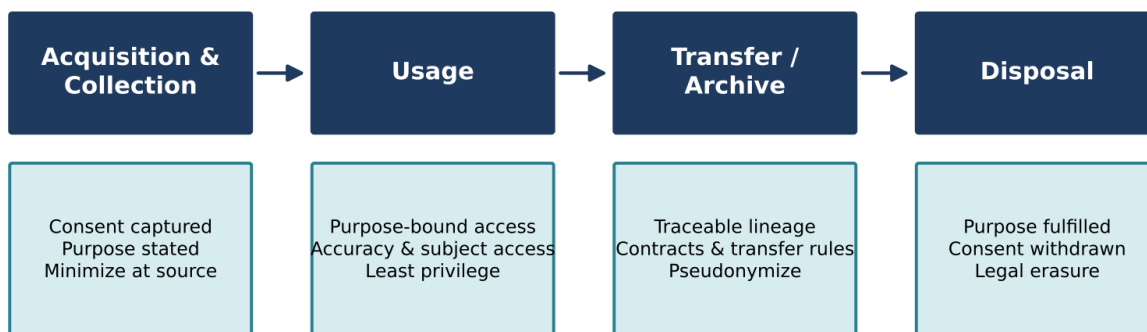


Figure 3: The four stages of the personal data life cycle

4.1 Acquisition and collection

- Collection of PII by a controller requires a lawful basis, typically consent from the user (the data subject) of an application, service or website.
- The data subject must be able to restrict the use of their data.

4.2 Usage

- Data must remain consistent while stored, even when provided or transferred to another controller.
- The data subject must have secure access, so they can verify and update their data.

4.3 Transfer or archival

- When data moves to another area of data responsibility, the transfer is carried out so that the data remains traceable to the data subject (for rights requests and corrections).
- Where data is retained for secondary purposes such as statistical research, it is pseudonymized or anonymized so it can no longer be traced back to the data subject.

4.4 Disposal

Disposal occurs when:

- The data is no longer required for the purposes for which it was collected;
- The data subject withdraws consent;
- There are no longer legal grounds for processing; or
- Erasure is required to comply with local law.

4.5 Controls by life cycle stage

Table 10: Controls and evidence by life cycle stage

Stage	Key PbD requirements	Typical controls	Evidence for the ARB
Acquisition and collection	Purpose specification; lawfulness; minimization; transparency	Consent capture; just-in-time notice; schema-level field minimization; classification at ingest	Consent records; data inventory; notice text
Usage	Purpose limitation; accuracy; security; intervenability	Purpose-based access control; read-only views; masking; self-service access and correction	Access policies; access logs; DSR test results
Transfer or archival	Purpose limitation; security; accountability	Data processing agreements; transfer mechanisms; pseudonymization; lineage tagging	Records of processing; lineage graph; contracts
Disposal	Storage limitation; security	Retention schedules; automated deletion including backups; cryptographic erasure; certificates of destruction	Retention configuration; deletion job logs

5. PbD Across the Enterprise Architecture

PbD cannot be implemented in silos. It must be carried out end to end, across the Customer Journey and across architectural layers, collaboratively between domains. This section gives the method for doing so and connects it to the data-centric architecture used in the Enterprise Architecture M&A Integration Playbook.

5.1 Five steps toward a PbD-compliant E2E architecture

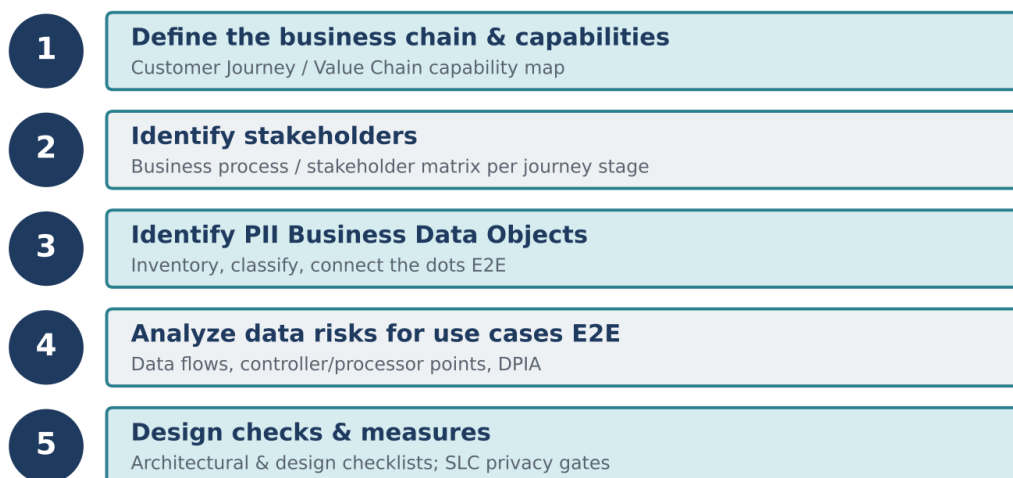


Figure 4: Five steps toward a PbD-compliant end-to-end architecture

Step 1. Define the business chain and capabilities

Start from the E2E Customer Journey and Value Chain capability map (Innovation and forecasting, Discover, Explore, Evaluate, Buy, Implement, Adopt, Expand/Migrate, Renew) and the subsystems that support each stage. Section 5.3 marks the capabilities that typically process personal data, which become the scope of the privacy analysis.

Step 2. Identify stakeholders

Build the business process / stakeholder matrix: for each stakeholder, the journey stages where it runs business processes. A business process is a sequence of actions performed by a specific stakeholder on BDOs to achieve a specific business result. Every stakeholder with an “X” handles data and must own the privacy controls for its processes (section 5.4).

Step 3. Identify and analyze PII Business Data Objects

- **Inventory** reference data, master data and business-chain transaction data.
- **Categorize** each BDO and attribute using the Enterprise classification scheme (Table 15).
- **Connect the dots E2E:** understand the BDO referential patterns, and determine the controller and processor points where responsibility for the data changes.

Table 11: Enterprise data classification scheme

Classification	Description	Examples	Minimum handling
Public	Approved for public release	Published product information, public price lists	Integrity controls

Classification	Description	Examples	Minimum handling
Internal	For Enterprise use; low impact if disclosed	Org charts, internal procedures	Authentication; internal access only
Confidential	Business-sensitive; may include personal data under GDPR, CCPA/CPRA, LGPD, etc.	Customer contact and account data, order history, user IDs	Role-based access; encryption at rest and in transit; logging; retention schedule
Restricted	Highest sensitivity; may include special-category or sensitive personal data	Health, biometric, government ID, payment data, precise location, children's data	Need-to-know access; strong authentication; field-level encryption or tokenization; DPIA required; segregated storage

Step 4. Analyze data risks for use cases E2E

Trace the data flows of each Customer Journey use case across systems and stakeholders, and assess privacy risk at every hand-off. The core use cases are the same as in the M&A playbook:

1. Customer acquires Rights to use or consume a product, content or service, directly or via a co-seller or embedded (OEM) partner.
2. Customer activates the product or service as permitted by the Rights.
3. Customer uses the product or service, including events outside compliance and grace rules, reported across the whole licensing life cycle.
4. Customer acquires add-on Rights for an existing subscription.
5. Customer renews subscription or term Rights.
6. Customer requests, and receives, support on an activated product instance.

For each use case, record the personal data BDOs touched, the purpose and lawful basis, the controller and processor at each step, cross-border transfers, retention, and the residual risk after controls. Record application and data-flow relationships in the EA repository so that privacy impact can be queried by application, BDO or interface.

Step 5. Design checks and measures

Apply the architectural checklist (section 7) and design checklist (section 8) to the risks found, and evidence the results at the SLC privacy gates (section 10).

5.2 The privacy-aware layered view

To avoid silos, the EA practice analyzes and designs on two dimensions: architectural **layers** crossed with the **E2E Customer Journey**. Business Data Objects and their data flows are the central layer: personal data is a property of BDOs, so privacy is designed at the BDO level and then realized in the layers above and below.

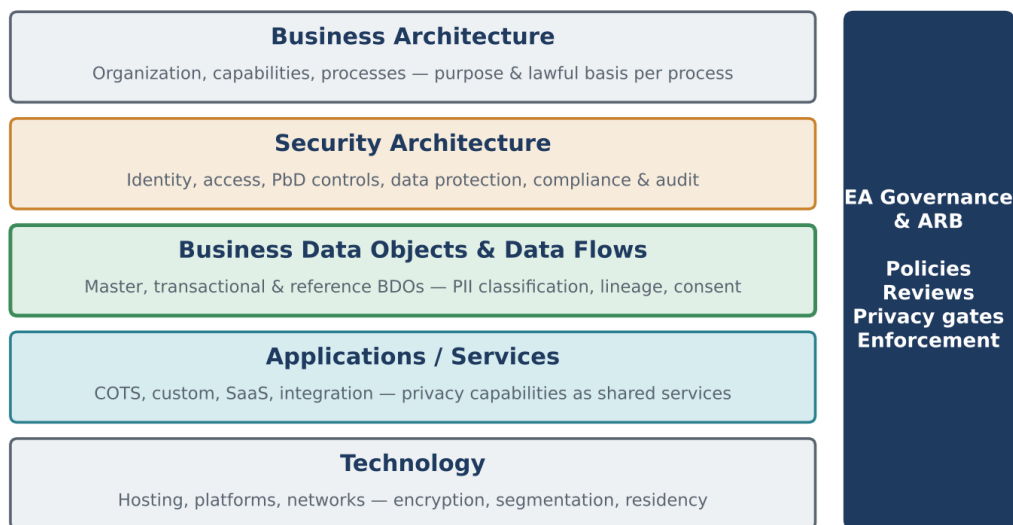


Figure 5: Privacy-aware, BDO-centric enterprise architecture stack

Table 12: Privacy concerns by architectural layer

Layer	Privacy concerns	Typical artefacts
Business	Purpose and lawful basis for each process; stakeholder accountability; notices	Capability map; process/stakeholder matrix; records of processing
Security	Identity, access, PbD controls, data protection, compliance and audit	Access model; threat model; control catalog
BDOs and data flows	Which BDOs and attributes are personal; classification; lineage; consent and purpose tags	Logical data model with classification; data-flow diagrams; data inventory
Applications and services	Which applications master or copy personal data; use of shared privacy services	Application landscape; interface catalog; DPIA
Technology	Encryption, segmentation, residency, logging, backup and disposal	Hosting and region map; key management design; retention configuration
EA governance	Policy, review and enforcement across all layers	ARB decisions; exceptions register; gate evidence

5.3 Privacy touch points across the Customer Journey

The capability map below follows the Customer Journey. For each subsystem it lists the personal data typically processed and the PbD concerns the architecture must address. Use it as a heat map during analysis: green where Enterprise privacy services already cover the capability, amber where they need extension, red where they are missing.

Table 13: Privacy touch points across the Customer Journey capability map

Subsystem (journey stage)	Personal data typically processed	Key PbD concerns
Offer management (NPI)	Eligibility rules referencing customer attributes; trial and redemption records	Minimize attributes used for eligibility; avoid sensitive attributes in targeting

Subsystem (journey stage)	Personal data typically processed	Key PbD concerns
Marketing (Discover, Explore)	Leads, contact details, behavioral and campaign data, preferences	Consent and preference management; central unsubscribe; tracking off by default; personalization transparency
Sales (Evaluate, Buy)	Accounts, contacts, opportunities, partner-relationship data	Purpose limitation between sales and marketing use; partner data-sharing agreements
Order management (Buy)	Purchaser identity, addresses, payment method references, tax data	Tokenized payment data; trade-compliance screening scope; retention of order records
Contract management (Buy)	Customer Rights, subscriptions, usage and consumption records	Link usage to Rights without unnecessary user-level detail; aggregation for compliance reporting
Authorization (Implement)	Activation events, device identifiers, delegated users	Minimize device fingerprinting; scope of delegated visibility
Customer admin (Implement, Adopt)	User directory, roles, deployment data	Least privilege for administrators; federated identity; admin audit trail
Payment management (Adopt)	Measured usage, payment instruments, collections	Payment data segregation and tokenization; usage aggregation before billing
Revenue and financial (Adopt, Renew)	Billing records, royalties, financial reporting	Pseudonymized or aggregated data for analytics; legal retention periods
Customer service (Expand, Renew)	Cases, chat and telephony transcripts, remote-support sessions, community posts	Recording notice and consent; redaction of transcripts; support-agent access scoping; retention
Core: business support, IT, HR, legal	Master data, identity, employee data, litigation holds	Master data stewardship; identity management; HR data segregation; legal-hold override of deletion

5.4 Stakeholders and privacy accountability

Every stakeholder has processes that support the life cycle, so every stakeholder must be engaged. The matrix records where each stakeholder acts on personal data and its main privacy accountability.

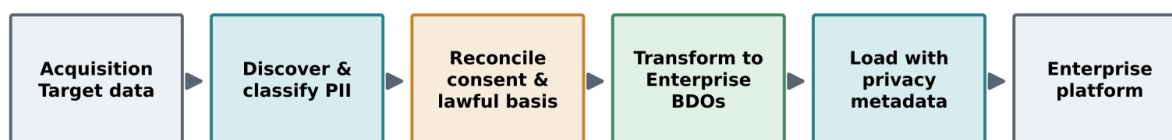
Table 14: Stakeholder privacy accountability

Stakeholder	Journey stages touched	Primary privacy accountability
Privacy Office (CPO)	All	Policy, legal interpretation, DPIA approval, regulator liaison
Enterprise Architecture / ARB	All	PbD architecture standards, gate reviews, exceptions
IT / platform engineering	All	Shared privacy services, security controls, retention and deletion
Product / business unit	NPI to Customer Service	Purpose definition, privacy requirements, default settings
Quote-to-cash operations	Marketing to Finance	Order and contract data handling, data quality
Finance	NPI, Sales to Customer Service	Billing and revenue data, legal retention

Stakeholder	Journey stages touched	Primary privacy accountability
Support	All	Case data minimization, transcript redaction, remote-session controls
Data and analytics	Most stages	De-identification, aggregation, analytics purpose limitation
Sales and sales operations	NPI, Sales to Customer Service	CRM data quality and purpose limitation
Marketing	Most stages	Consent, preferences, tracking, personalization
Entitlement / license compliance	Sales to Payment	Usage data minimization; aggregation for true-up
Channel management and partners	Marketing to Customer Service	Data-sharing agreements, partner isolation of customer data
OEM partners and IP providers	Varies	Processor/sub-processor obligations; contractual safeguards
Customer	Marketing onward	Exercises rights and consent choices; administers delegated users

5.5 PbD in M&A integration

Acquisitions concentrate privacy risk. The Acquisition Target's personal data was collected under its own notices, consents and lawful bases, which may not cover processing in the Enterprise. Migration must therefore carry privacy metadata as well as the data itself.



**Quarantine records whose consent or lawful basis cannot be proven.
Never merge inherited PII before its permissions are reconciled.**

Figure 6: Privacy-aware migration of inherited personal data

- **During due diligence**, request the Target's records of processing, privacy notices, consent records, data processing agreements, cross-border transfer mechanisms, breach history and DPIAs.
- **Classify** the Target's data with the Enterprise scheme (Table 15) and map it to Enterprise BDOs before any merge.
- **Reconcile permissions**: for each data set, confirm that the purpose and lawful basis under which it was collected cover its intended use in the Enterprise. Where they do not, obtain fresh consent, re-notify, restrict use, or exclude the data.
- **Migrate privacy metadata** (consent state, purpose tags, retention clock, data subject request history, suppression lists) as reference data alongside master and transactional data.

- **Quarantine** records whose consent or lawful basis cannot be proven; do not merge them into consolidated customer profiles.
- **Honor in-flight obligations:** open data subject requests, opt-outs and deletion commitments made by the Target carry over and must be fulfilled on the Enterprise platform.
- **Retire legacy stores** under the Enterprise retention schedule once open transactions have aged out, with documented secure disposal.

6. Requirements Checklists

6.1 Enterprise privacy principles review

- Have the Enterprise privacy principles, as published by the Privacy Office, been applied to the initiative?
- Has the privacy engineering review team examined the pre-requirements and requirements below in the project's context, and verified or added to them for the specific product?

6.2 Pre-requirement checklist

Define the processing to be done and establish an overview of the personal data:

- Will the software process personal data?
- Identify the controller and any processors and sub-processors. Processing contracts must be signed, and sub-processors approved by the controller.
- What is the legal basis for the processing?
- What is the purpose of the processing?
- For how long do the legal basis and the purpose allow personal data to be stored? Is automatic erasure needed?
- Define the categories of personal data necessary to achieve the purpose. Processing of special categories of personal data, and of data relating to criminal convictions and offences, is generally prohibited with limited exceptions; determine whether an exception applies. Document the full scope of data stored by the software.
- How is transparency achieved: automatic notifications, a privacy dashboard, notices?
- Is personal data transferred to a third country or an international organization? If so, confirm that every transfer is lawful and that restrictions on access, operations and storage are met.
- In what context will the processing take place, and could the software be used in another context?
- Which requirements apply to the business: sector codes of conduct, internal policies, contractual commitments?
- Are there certification schemes the software can and should follow, and what do they require?
- Has a data protection authority made decisions in this field, about the Enterprise or comparable businesses, that should become requirements?

6.3 Requirements for data protection and information security

- If the software works as intended without identifiable data, no identifying data may be collected.
- Design data protection in using pseudonymization techniques.
 - Unnecessary identification and redundant personal data increase risk to the data subject and make the software more vulnerable and more attractive to actors wishing to reuse the data for other purposes.
- The software uses personal data only as planned, and deletes it when storage is no longer lawful or necessary for the purpose.
- Personal data is available to those authorized to use it when needed.
- Default settings protect the rights of data subjects and safeguard privacy.

- The software guides users to the most privacy-friendly manner of use; for example, location sharing is disabled by default and can be enabled by the user.

6.4 Requirements for meeting data protection principles

Lawfulness, fairness and transparency

Processing of personal data is lawful only if at least one of these applies:

- the data subject has given consent;
- processing is necessary to perform a contract with the data subject;
- processing is necessary to comply with a legal obligation;
- processing is necessary to protect the vital interests of the data subject or another natural person;
- processing is necessary for a task carried out in the public interest or in the exercise of official authority;
- processing is necessary for the legitimate interests of the controller, subject to a balancing of interests.

In addition:

- Processing is predictable to the data subject and respects their interests.
- Relevant aspects of processing are known to the data subject, so they can make informed decisions and exercise their rights.
- Other rights, such as freedom of expression, freedom of thought, freedom of religion and non-discrimination, are safeguarded.
- Clear, comprehensible information is provided about the purpose, the legal basis and the recipients of the data.

Purpose limitation, minimization, accuracy, storage limitation, integrity

Principle	Requirement
Purpose limitation	Collect personal data only for specified, explicit and legitimate purposes, and do not further process it in a manner incompatible with them.
Data minimization	Process only personal data that is adequate, relevant and limited to what is necessary for the purposes.
Accuracy	Keep personal data accurate and up to date; delete or rectify incorrect data.
Storage limitation	Ensure the data subject cannot be identified for longer than strictly necessary for the purposes.
Integrity and confidentiality	Ensure appropriate security of the personal data (section 6.7).

If processing is based on consent

- Consent is explicit (not passive), voluntary (no coercion or pressure) and informed (predictable).
- Processing based on consent is clearly distinguished from other matters.
- The declaration of consent is in clear, plain language at the reader's level, intelligible and easily accessible. Separate conditions apply to children's use of online services.
- Users can withdraw consent at any time, as easily as they gave it.

6.5 Requirements to protect the rights of the data subject

The information obligation differs depending on whether data is obtained from the data subject or from another source. When obtained from the data subject, they must be told:

- the identity and contact details of the controller, and of the data protection officer where relevant;
- the purposes of the processing and its legal basis;
- the legitimate interests pursued, where processing relies on a balancing of interests;
- the recipients, including processors;
- whether data will be transferred to a third country or international organization.

Where necessary for fair and transparent processing, they must also be told:

- how long the data will be stored;
- their rights of access, rectification and erasure, to object and to restrict processing, and to data portability;
- that consent can be withdrawn at any time;
- whether provision of the data is a contractual requirement or necessary to enter a contract;
- whether the software involves automated decision-making or profiling, with meaningful information about the logic involved and its significance and consequences;
- whether the data will be used for purposes other than those for which it was collected, and which rights and rules apply.

When data is collected from someone other than the data subject, they must also be told the categories of personal data processed and the source, including whether it came from publicly accessible sources.

The software must make it easy for data subjects to exercise their rights:

- access to their personal data and information about the processing;
- rectification, as quickly as possible;
- erasure, as quickly as possible, where the conditions apply (the “right to be forgotten”);
- restriction of processing, where the conditions apply;
- data portability, where processing is based on consent or contract and carried out by automated means;
- objection to processing, where the preconditions are met;
- rights relating to automated individual decision-making, including profiling, with legal or similarly significant effects.
- When data is rectified, erased or restricted at the data subject’s request, the controller informs every recipient to whom it was disclosed.
- The software pseudonymizes personal data when identification is no longer needed, and anonymizes or deletes it when the purpose is fulfilled.
- The software prevents linking of personal data about a data subject to personal data in other systems, or collected for other purposes.

6.6 Requirements to fulfil the organization’s obligations

When using processors:

- Use only processors that give adequate guarantees of measures ensuring compliance with data protection law and protection of data subjects’ rights.

- Ensure suppliers and sub-processors meet all requirements by entering into processing contracts.

6.7 Security of processing (C-I-A-R-T)

Security of processing requires **confidentiality (C)**: protection against unauthorized disclosure or access; **integrity (I)**: protection against accidental or unlawful destruction, loss or alteration; and **availability (A)**: access for authorized personnel who need it. Data protection law also requires **resilience (R)**, the ability to resist vulnerabilities, attacks and accidents, and this playbook adds **traceability (T)**, documentation of changes to the software and to personal data so that breaches can be managed.

Table 15: Security requirements and the C-I-A-R-T properties they serve

Area	Requirement	C-I-A-R-T
Access control	Users are identified	T
	Roles and rights follow the principle of least privilege	A
	Traceability can be verified by auditing logs	T
	Users access only the information needed for their tasks	C, T
	Administrator privileges are limited to a small number of individuals	C, I, A, R, T
	Data subjects can access their own personal data	I, A
	Passwords are handled securely and must be strong	C, I, A
	Strong (multi-factor) authentication where necessary; required for administrators and users with access to sensitive or bulk personal data	C, I, T
	Attempts at unauthorized access are monitored	C, I, R, T
	Third-party access is restricted and limited (e.g. specified IP ranges, temporary scoped access)	C, I, R
Encryption	Recognized algorithms and adequate key lengths, reviewed on a defined schedule, for: endpoints; remote access; transfer and storage in cloud services; backups and backup media	C, A, R
Integrity	Detect changes in files, servers and networks by hash and checksum comparison, limited write access, regular integrity checks and reference values	I
Availability	Redundancy, contingency plans and incident management; timely restoration of availability and access after a physical or technical incident	A
Resilience	Secured against known vulnerabilities; correctly configured; segmentation of data, systems, processors and networks; third-party software and patches kept current; vulnerability reports received and managed; secure destruction of media	R
Traceability	Documented software and procedures; logging of configuration changes, processes, activities and incidents; least-privilege access to logs; logs deleted or anonymized after a set period and not kept longer than necessary	T

6.8 Acceptable level of risk

- Establish tolerance levels for data protection and for information security, defining acceptable risk for the software, based on established supporting tables and tolerance limits. The methodology can be reused across initiatives.

- Use auxiliary tables to categorize criticality (e.g. Critical, High, Moderate, Low), with variables and an acceptable level of risk for each category.

Table 16: Outcomes that require an acceptable level of risk

Data protection outcomes requiring a defined risk tolerance	Security outcomes requiring a defined risk tolerance
The data subject keeps control of their personal data	No accidental or unlawful destruction, loss or alteration of personal data
The data subject does not lose rights or freedoms	No unauthorized disclosure of, or access to, personal data
The data subject is not profiled or discriminated against	Confidentiality, integrity, availability and resilience are secured
The data subject is not exposed to identity theft or fraud	Personal data is pseudonymized as early as possible and encrypted
The data subject suffers no financial or reputational loss	Availability and access can be restored in a timely manner after an incident
Pseudonymized data cannot be re-identified without authorization	Effectiveness of security measures is regularly tested, assessed and evaluated
No confidentiality breach of protected data occurs	

7. Architectural Checklist: the Eight Privacy Design Strategies

Many business analysts and product managers are not fully aware of the personal data requirements the Privacy Office defines. Those requirements must be understood and built into the functional requirements of every project or program. The eight strategies below are the ARB's architectural checklist. Four are **data-oriented** (Minimize, Hide, Separate, Aggregate) and four are **process-oriented** (Inform, Control, Enforce, Demonstrate).

7.1 Strategy 1: Minimize

- The amount of personal data processed is restricted to the minimum possible.
- By collecting no unnecessary data, the possible privacy impact of a system is limited.
- Applying Minimize means answering whether processing is proportional to the purpose, and whether a less invasive means exists to achieve the same purpose.

ARB question: Can each personal data attribute be justified against a stated purpose, and has a less invasive alternative been considered?

7.2 Strategy 2: Hide

- Personal data, and their interrelationships, are hidden from plain view, so they cannot easily be abused.
- Seemingly innocuous identifiers can later turn out to be privacy problems; Hide forces designers to rethink their use.
- Hide aims for unlinkability and unobservability.

ARB question: Where is personal data visible in clear text, and which identifiers could link records across contexts?

7.3 Strategy 3: Separate

- Personal data is processed in a distributed fashion, in separate compartments, whenever possible.
- Separating processing or storage of several sources of data about the same person prevents complete profiles from being built.
- Prefer distributed to centralized processing; store data from separate sources in separate, unlinked databases; process and store locally where possible.
- Split database tables, and make rows hard to link, for example by removing identifiers or using table-specific pseudonyms.

ARB question: Could a single compromise or query assemble a complete profile of an individual?

7.4 Strategy 4: Aggregate

- Personal data is processed at the highest level of aggregation, with the least detail at which it is still useful.
- Aggregation over groups of attributes or individuals restricts the remaining detail.
- Data is less sensitive if it is coarse-grained and the aggregated group is large enough.
- Coarse-grained data is valid for many individuals, so little can be attributed to any one person.

ARB question: Is individual-level data used where aggregate data would meet the purpose?

7.5 Strategy 5: Control

- Data subjects have agency over the processing of their personal data.
- Control is the counterpart to Inform: without reasonable means of control, there is little point in informing.
- It governs whether users choose to use a system and how they control what is processed about them.
- Data subjects are informed of their access rights and how to exercise them.

ARB question: Can a data subject see, change, export, restrict and delete their data, and withdraw consent, without contacting support?

7.6 Strategy 6: Inform

- Corresponds to transparency (principle 6, Visibility and Transparency).
- Data subjects are adequately informed whenever personal data is processed.
- When using a system, they are told what information is processed, for what purpose and by which means.
- They are told about third parties with which information is shared.

ARB question: At the moment of collection, does the individual know what is collected, why, for how long and who else receives it?

7.7 Strategy 7: Enforce

- A privacy policy compatible with legal requirements is in place and enforced.
- The level of protection depends on the policy requirements.
- Technical mechanisms prevent violations of the privacy policy.
- Governance structures to enforce the policy are established.

ARB question: Which policy rules are enforced by the system itself, rather than by procedure alone?

7.8 Strategy 8: Demonstrate

- The data controller can demonstrate compliance with the privacy policy and applicable law.
- The controller can show how the policy is implemented within the IT or cloud capability or solution.
- After a complaint or incident, the extent of any breach can be determined immediately.

ARB question: What evidence could be produced tomorrow for an auditor, regulator or data subject?

8. Design Checklist

8.1 Data-oriented design requirements

Minimize and limit

Limit personal data collected and processed to what is lawful and strictly necessary, and delete it when no longer needed for the purposes. Follow the principle **select before you collect**.

- Execute and review a data protection impact assessment (DPIA).
- Match the amount and scope of data collected to the need; collect nothing more.
- Limit information processed on devices or in areas with lower trust and security assurance.
- Avoid, limit or minimize the collection and processing of sensitive personal data.
- Minimize exposure of unnecessary functionality and personal data in the user interface. Consider whether directly identifying information must be stored at all, or whether pseudonymized information suffices.

Hide and protect

Do not communicate, process or store personal data and their interrelationships in plain view. Hiding directly identifiable data significantly reduces the risk of abuse and the scope of incidents. Techniques include pseudonymization, encryption and aggregation.

- Conduct threat modelling and attack surface analysis during design (section 8.3).
- Use encryption for transfer, communication, processing and storage, particularly across uncontrolled networks.
- Anonymize or pseudonymize personal data wherever possible.
- Avoid unnecessary exposure of communication patterns and connection points (APIs, feeds, gateways, login interfaces).

Separate

Separate personal data from other data where possible, storing it in separate databases, entities and areas for each purpose and process. Separation limits profiling, supports purpose limitation and reduces linkability. Tables containing personal data should have shorter retention and automatic deletion deadlines; tables without personal data may be kept longer. Measures include table-level access control, split tables, and separation of high-trust and low-trust components.

- Separate sensitive from less sensitive personal data (in databases, site access, clients and devices).
- Separate tables, with access rights to tables and areas granted by job necessity (least privilege).
- Keep less trusted units and areas separate from more trusted ones.
- Make rows in tables hard to link to one another.

Aggregate

Gather and process personal data in as aggregated a form as possible, without prejudice to the business value and purpose.

- Reduce the use of detailed and sensitive personal data.
- Remove unnecessary and excessive detail, for example:
 - use weeks rather than days or hours;

- use counties or regions rather than street addresses;
- use groups rather than individuals.
- Use anonymization techniques wherever possible.

Data protection by default

Configure every setting in its most privacy-friendly state by default. The user must make a conscious choice to change a setting that reduces privacy, such as sharing more data with others.

- All privacy-friendly configurations are on by default.
- Device tracking is disabled by default.
- Bluetooth and similar proximity features are disabled by default.
- Cross-site tracking is disabled by default.
- By default there is no reuse of information about which websites the data subject has visited.

8.2 Process-oriented design requirements

Inform

Design and configure the software so the data subject is sufficiently informed about how it works and how personal data is processed, including how any profiling or automated processing is done. Special requirements apply to software aimed at children. Before use, publish information about the software and provide:

- a point of contact or contact form for requests about the purpose and need for collection, the security of the software, and the use of sub-processors and sharing of data with them;
- multiple approaches and channels, to reach all user groups;
- simple, comprehensible language, in multiple languages where necessary;
- imagery, icons, audio and video suited to the target users.

Control

Data subjects have the right to control their own personal data, including requesting to view, update and delete it, and to demand human processing where decisions are automated. Design so these rights can be exercised as easily as possible. Establish the ability to:

- maintain an overview of which processing is necessary to fulfil the contract and which is subject to voluntary consent;
- give consent on an information page with a checkbox before using the software;
- withdraw consent from a menu within the software, ceasing collection immediately on withdrawal;
- rectify, block or delete personal data, for example by viewing collected data directly in the software;
- permanently delete personal data in the database and wherever else it is stored, including backups; or export it for manual review with a procedure to correct, block or delete it within 30 days;
- terminate an agreement, and install, uninstall, enable or disable an application, service, component or system, through a menu, a dedicated page or a form;
- submit questions or complaints about data protection and security, through the software or a staffed channel with a documented procedure;
- object to profiling and redistribution of personal data, for example by a checkbox that sets a stored flag, or through a staffed channel;

- understand how automated decisions are made and demand manual processing, as described in the system documentation and on an information page in the software.

Enforce

Design the software so it can document how it enforces data subjects' rights, including accountability and how data protection law is enforced, available for audit and inspection. This includes artificial intelligence, profiling and automated processing.

- Apply the highest privacy settings by default:
 - present settings in a menu where the user must consciously change to less privacy-friendly options;
 - if a later change makes settings less privacy-friendly, inform the user clearly and let them consent by checkbox after reading the notice.
- Meet the data portability requirement:
 - let the data subject obtain their personal data, or have it transferred to another provider, in a structured, commonly used, machine-readable format;
 - this right applies where processing is based on consent or contract;
 - deliver exports securely to the data subject or a new provider.
- Require active participation for consent:
 - consent or change of consent is signaled by an affirmative action that sets a flag in the database;
 - software aimed at minors requires verified consent from a parent or guardian before access, or a documented manual consent procedure.
- Give the data subject an overview of what access has taken place (including their own), when, by whom, and what consent has been given, from logs that can be made available to them.

Demonstrate

The controller must be able to document compliance with data protection law and the security of processing. Design and develop the software so the controller can show how each requirement was implemented. Evidence includes documentation that a secure software development life cycle (SSDLC) with data protection by design was followed, security audit reports, vulnerability scans, penetration test results and records of breach-management exercises.

8.3 Attack surface analysis and threat modelling

Analyze and reduce the attack surface

- Analyze the attack surface of the designed software to reduce opportunities to exploit weaknesses.
- Review where the design receives input, produces output, and transports and stores data.
- Check whether the same information is collected in several places (duplicate functionality) and simplify.
- Reduce the likelihood of errors by removing unnecessary functionality.
- Reuse the security risk and data protection impact assessments from the requirements phase, and their tolerance levels.
- Where existing levels are not acceptable, implement vulnerability-reducing measures to reach tolerance.
- Document the analysis and the reduction achieved.

Threat modelling

- Analyze components, access points, data flows and processing.
- Have the development team analyze how the software could be misused in different scenarios.
- Review each scenario and improve the design to avoid identified threats with vulnerability-reducing measures.
- Risk-assess any remaining vulnerabilities, mitigate them by other measures, and record them in the risk log.

Tools and techniques

Table 17: Design tools and techniques

Technique	Use
Security design principles	Least privilege; defense in depth; fail securely
Threat modelling (STRIDE)	Systematic security threats: spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege
Privacy threat modelling (LINDDUN)	Privacy threats: linking, identifying, non-repudiation, detecting, data disclosure, unawareness, non-compliance
DREAD	Ranking threats by damage, reproducibility, exploitability, affected users and discoverability
Attack surface analysis	Enumerating entry points, exit points and data stores
Use-case and misuse-case modelling	Pairing intended behavior with abuse scenarios
Attack trees	Decomposing an attacker goal into the paths that achieve it

8.4 Why design requirements are necessary

- Personal data must be processed lawfully, and the software design must reflect this (GDPR Article 6 and equivalents). Teams must know the types of personal data processed, the purpose and terms of processing, and how data is compiled.
- The rights of the data subject must be reflected in the design (GDPR Articles 12–23 and equivalents).
- Privacy defects found after release cost far more to fix than those prevented in design, and some, such as unlawful collection, cannot be fixed retrospectively at all.

9. Enterprise Privacy Capabilities

Few off-the-shelf enterprise-wide privacy products exist; a complete solution usually combines third-party point solutions with internal IP. To avoid every application building its own, the Enterprise provides privacy capabilities as **shared services** consumed through standard APIs and events. Each capability below should have a named owner, an API contract and a BDO model in the EA repository. Projects must use them where they apply; exceptions require ARB approval.

Table 18: Reference Enterprise privacy capabilities

Capability	What it provides	PbD strategies served
Consent and preference management	Capture, store and propagate consent and communication preferences by purpose and channel; full consent history; withdrawal propagated to all subscribers	Control; Inform; Demonstrate
PII inventory and tracking	Enterprise inventory of where personal data lives, its classification, purpose, lineage and retention; queryable by system, BDO or data subject (for example, a PII-tracking service such as PII-Track)	Demonstrate; Enforce
Data subject request (DSR) orchestration	Intake, identity verification and fan-out of access, correction, deletion, portability and objection requests to all systems; tracking to closure within statutory deadlines	Control; Demonstrate
Data discovery and classification	Scanning of structured and unstructured stores to find and tag personal data; drift detection for untagged PII	Minimize; Enforce
De-identification and tokenization	Pseudonymization, tokenization, masking, aggregation and privacy-preserving analytics as a service	Hide; Aggregate; Separate
Retention and deletion	Retention schedules by data category; automated deletion across primary stores, replicas and backups; legal-hold override	Minimize; Enforce
Purpose-based access control	Access decisions that combine role with declared purpose and data classification	Enforce; Separate
Privacy audit and evidence	Immutable logging of access and processing events; records of processing; reports for audits and data subjects	Demonstrate; Inform
Notice management	Versioned privacy notices linked to the processing they describe and to the consents given under each version	Inform; Demonstrate

For each initiative, record which capabilities it consumes, which it extends, and any gap it exposes, using the same green/amber/red heat-map approach as section 5.3.

10. ARB Governance and Review Gates

PbD is executed through the Enterprise service life cycle (SLC) process model. The ARB and the Privacy Office review privacy at defined milestones. Execution may augment the SLC fundamentals where needed for an enterprise solution; the SLC itself is executed in the context of this playbook and the ARB guidelines.

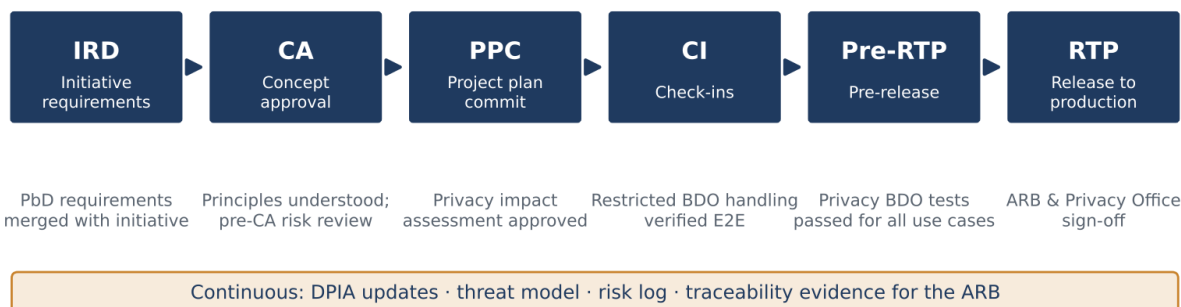


Figure 7: Privacy milestones in the service life cycle

Table 19: SLC privacy milestones and evidence

Milestone	PbD objective	Evidence required
IRD: initiative requirements	Privacy Office requirements merged with initiative requirements	Pre-requirement checklist (6.2); initial data inventory; legal basis and purpose per processing activity
CA: concept approval	PbD principles understood by solution architects; high-level risks defined in a pre-CA review	Five-step analysis Steps 1–3 (5.1); classification of BDOs; initial risk assessment
PPC: project plan commit	Privacy impact assessment presented to and approved by the ARB and Privacy Office	DPIA; E2E data-flow diagrams (Step 4); architectural checklist (section 7); capability consumption plan (section 9)
CI: check-ins	ARB works with solution architects to check restricted BDO identification, collection, storage, use, processing and referential checks	Design checklist (section 8); threat model; updated risk log
Pre-RTP: pre-release	Testing meets privacy BDO requirements for all use cases tested E2E, including usage, sharing and retention	Privacy test results (consent, DSR, deletion, defaults); penetration test; residual risk acceptance
RTP: release to production	ARB review for alignment with the PPC architecture; Privacy Office sign-off on RTP ARB check	Gate sign-off; records of processing updated; operational runbooks for breach and DSR

10.1 Exceptions

Where a project cannot meet a requirement, it records an exception with the risk, compensating controls, owner and expiry date. The ARB approves or rejects exceptions jointly with the Privacy Office, and the exceptions register is reviewed at every subsequent gate until closed.

10.2 Conclusion

An unprepared Enterprise faces real risk in protecting personal data. PbD cannot be implemented in silos; it must be carried out end to end across the Customer Journey, collaboratively between domains. There are few off-the-shelf enterprise-wide solutions, so a thorough approach relies on combining point solutions with internal capabilities governed by a common architecture. When the Enterprise adheres to the seven foundational principles and applies the strategies, checklists and gates in this playbook, the benefits are considerable: lower risk, faster compliance with new regulation, reusable capabilities, and the trust of customers and partners.

Appendix A. NIST Privacy Framework Core Functions

The U.S. Department of Commerce National Institute of Standards and Technology (NIST) Privacy Framework Version 1.0 (January 2020) organizes privacy outcomes into five functions. The Core is reproduced below as a reference for coverage checks. NIST has since published Version 1.1, which realigns the Framework with the NIST Cybersecurity Framework 2.0 and adds guidance on AI; teams should confirm which version their program has adopted and use NIST's published 1.0-to-1.1 mapping where needed.

A.1 IDENTIFY-P (ID-P)

Function: Develop the organizational understanding to manage privacy risk for individuals arising from data processing.

Category	Subcategory
Inventory and Mapping (ID.IM-P): Data processing by systems, products or services is understood and informs the management of privacy risk.	ID.IM-P1: Systems/products/services that process data are inventoried.
	ID.IM-P2: Owners or operators (e.g. the organization or third parties such as service providers, partners, customers and developers) and their roles with respect to the systems/products/services and components (e.g. internal or external) that process data are inventoried.
	ID.IM-P3: Categories of individuals (e.g. customers, employees or prospective employees, consumers) whose data are being processed are inventoried.
	ID.IM-P4: Data actions of the systems/products/services are inventoried.
	ID.IM-P5: The purposes for the data actions are inventoried.
	ID.IM-P6: Data elements within the data actions are inventoried.
	ID.IM-P7: The data processing environment is identified (e.g. geographic location, internal, cloud, third parties).
	ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.
Business Environment (ID.BE-P): The organization's mission, objectives, stakeholders and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities and risk management decisions.	ID.BE-P1: The organization's role(s) in the data processing ecosystem are identified and communicated.
	ID.BE-P2: Priorities for organizational mission, objectives and activities are established and communicated.
	ID.BE-P3: Systems/products/services that support organizational priorities are identified and key requirements communicated.

Category	Subcategory
Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g. compliance, financial), reputation, workforce and culture.	ID.RA-P1: Contextual factors related to the systems/products/services and the data actions are identified (e.g. individuals' demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties).
	ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias.
	ID.RA-P3: Potential problematic data actions and associated problems are identified.
	ID.RA-P4: Problematic data actions, likelihoods and impacts are used to determine and prioritize risk.
	ID.RA-P5: Risk responses are identified, prioritized and implemented.
Data Processing Ecosystem Risk Management (ID.DE-P): The organization's priorities, constraints, risk tolerance and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess and manage privacy risks within the data processing ecosystem.	ID.DE-P1: Data processing ecosystem risk management policies, processes and procedures are identified, established, assessed, managed and agreed to by organizational stakeholders.
	ID.DE-P2: Data processing ecosystem parties (e.g. service providers, customers, partners, product manufacturers, application developers) are identified, prioritized and assessed using a privacy risk assessment process.
	ID.DE-P3: Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.
	ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.
	ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results or other forms of evaluations to confirm they are meeting their contractual, interoperability framework or other obligations.

A.2 GOVERN-P (GV-P)

Function: Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.

Category	Subcategory
----------	-------------

Category	Subcategory
Governance Policies, Processes and Procedures (GV.PO-P): The policies, processes and procedures to manage and monitor the organization's regulatory, legal, risk, environmental and operational requirements are understood and inform the management of privacy risk.	GV.PO-P1: Organizational privacy values and policies (e.g. conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated.
	GV.PO-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place.
	GV.PO-P3: Roles and responsibilities for the workforce are established with respect to privacy.
	GV.PO-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g. service providers, customers, partners).
	GV.PO-P5: Legal, regulatory and contractual requirements regarding privacy are understood and managed.
	GV.PO-P6: Governance and risk management policies, processes and procedures address privacy risks.
Risk Management Strategy (GV.RM-P): The organization's priorities, constraints, risk tolerances and assumptions are established and used to support operational risk decisions.	GV.RM-P1: Risk management processes are established, managed and agreed to by organizational stakeholders.
	GV.RM-P2: Organizational risk tolerance is determined and clearly expressed.
	GV.RM-P3: The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.
Awareness and Training (GV.AT-P): The organization's workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures and agreements and organizational privacy values.	GV.AT-P1: The workforce is informed and trained on its roles and responsibilities.
	GV.AT-P2: Senior executives understand their roles and responsibilities.
	GV.AT-P3: Privacy personnel understand their roles and responsibilities.
	GV.AT-P4: Third parties (e.g. service providers, customers, partners) understand their roles and responsibilities.
Monitoring and Review (GV.MT-P): The policies, processes and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.	GV.MT-P1: Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (e.g. introduction of new technologies), governance (e.g. legal obligations, risk tolerance), data processing, and systems/products/services change.
	GV.MT-P2: Privacy values, policies and training are reviewed, and any updates are communicated.

Category	Subcategory
	GV.MT-P3: Policies, processes and procedures for assessing compliance with legal requirements and privacy policies are established and in place.
	GV.MT-P4: Policies, processes and procedures for communicating progress on managing privacy risks are established and in place.
	GV.MT-P5: Policies, processes and procedures are established and in place to receive, analyze and respond to problematic data actions disclosed to the organization from internal and external sources (e.g. internal discovery, privacy researchers, professional events).
	GV.MT-P6: Policies, processes and procedures incorporate lessons learned from problematic data actions.
	GV.MT-P7: Policies, processes and procedures for receiving, tracking and responding to complaints, concerns and questions from individuals about organizational privacy practices are established and in place.

A.3 CONTROL-P (CT-P)

Function: Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

Category	Subcategory
Data Processing Policies, Processes and Procedures (CT.PO-P): Policies, processes and procedures are maintained and used to manage data processing (e.g. purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the organization's risk strategy to protect individuals' privacy.	CT.PO-P1: Policies, processes and procedures for authorizing data processing (e.g. organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place.
	CT.PO-P2: Policies, processes and procedures for enabling data review, transfer, sharing or disclosure, alteration and deletion are established and in place (e.g. to maintain data quality, manage data retention).
	CT.PO-P3: Policies, processes and procedures for enabling individuals' data processing preferences and requests are established and in place.
	CT.PO-P4: A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.
Data Processing Management (CT.DM-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g. individual participation, data quality, data minimization).	CT.DM-P1: Data elements can be accessed for review.
	CT.DM-P2: Data elements can be accessed for transmission or disclosure.
	CT.DM-P3: Data elements can be accessed for alteration.
	CT.DM-P4: Data elements can be accessed for deletion.

Category	Subcategory
	CT.DM-P5: Data are destroyed according to policy.
	CT.DM-P6: Data are transmitted using standardized formats.
	CT.DM-P7: Mechanisms for transmitting processing permissions and related data values with data elements are established and in place.
	CT.DM-P8: Audit/log records are determined, documented, implemented and reviewed in accordance with policy and incorporating the principle of data minimization.
	CT.DM-P9: Technical measures implemented to manage data processing are tested and assessed.
	CT.DM-P10: Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences.
Disassociated Processing (CT.DP-P): Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g. data minimization).	CT.DP-P1: Data are processed to limit observability and linkability (e.g. data actions take place on local devices, privacy-preserving cryptography).
	CT.DP-P2: Data are processed to limit the identification of individuals (e.g. de-identification privacy techniques, tokenization).
	CT.DP-P3: Data are processed to limit the formulation of inferences about individuals' behavior or activities (e.g. data processing is decentralized, distributed architectures).
	CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.
	CT.DP-P5: Attribute references are substituted for attribute values.

A.4 COMMUNICATE-P (CM-P)

Function: Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.

Category	Subcategory
Communication Policies, Processes and Procedures (CM.PO-P): Policies, processes and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g. purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks.	CM.PO-P1: Transparency policies, processes and procedures for communicating data processing purposes, practices and associated privacy risks are established and in place.
	CM.PO-P2: Roles and responsibilities (e.g. public relations) for communicating data processing purposes, practices and associated privacy risks are established.

Category	Subcategory
Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.	CM.AW-P1: Mechanisms (e.g. notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.
	CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g. surveys or focus groups) about data processing and associated privacy risks are established and in place.
	CM.AW-P3: System/product/service design enables data processing visibility.
	CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.
	CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g. data sources) in the data processing ecosystem.
	CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.
	CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event.
	CM.AW-P8: Individuals are provided with mitigation mechanisms (e.g. credit monitoring, consent withdrawal, data alteration or deletion) to address impacts of problematic data actions.

A.5 PROTECT-P (PR-P)

Function: Develop and implement appropriate data processing safeguards.

Category	Subcategory
Data Protection Policies, Processes and Procedures (PR.PO-P): Security and privacy policies (e.g. purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes and procedures are maintained and used to manage the protection of data.	PR.PO-P1: A baseline configuration of information technology is created and maintained incorporating security principles (e.g. concept of least functionality).
	PR.PO-P2: Configuration change control processes are established and in place.
	PR.PO-P3: Backups of information are conducted, maintained and tested.
	PR.PO-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.
	PR.PO-P5: Protection processes are improved.
	PR.PO-P6: Effectiveness of protection technologies is shared.

Category	Subcategory
	PR.PO-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place and managed.
	PR.PO-P8: Response and recovery plans are tested.
	PR.PO-P9: Privacy procedures are included in human resources practices (e.g. deprovisioning, personnel screening).
	PR.PO-P10: A vulnerability management plan is developed and implemented.
Identity Management, Authentication and Access Control (PR.AC-P): Access to data and devices is limited to authorized individuals, processes and devices, and is managed consistent with the assessed risk of unauthorized access.	PR.AC-P1: Identities and credentials are issued, managed, verified, revoked and audited for authorized individuals, processes and devices.
	PR.AC-P2: Physical access to data and devices is managed.
	PR.AC-P3: Remote access is managed.
	PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
	PR.AC-P5: Network integrity is protected (e.g. network segregation, network segmentation).
	PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g. individuals' security and privacy risks and other organizational risks).
Data Security (PR.DS-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity and availability.	PR.DS-P1: Data-at-rest are protected.
	PR.DS-P2: Data-in-transit are protected.
	PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers and disposition.
	PR.DS-P4: Adequate capacity to ensure availability is maintained.
	PR.DS-P5: Protections against data leaks are implemented.
	PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware and information integrity.
	PR.DS-P7: The development and testing environment(s) are separate from the production environment.
	PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.
Maintenance (PR.MA-P): System maintenance and repairs are performed consistent with policies, processes and procedures.	PR.MA-P1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.

Category	Subcategory
	PR.MA-P2: Remote maintenance of organizational assets is approved, logged and performed in a manner that prevents unauthorized access.
Protective Technology (PR.PT-P): Technical security solutions are managed to ensure the security and resilience of systems/products/services and associated data, consistent with related policies, processes, procedures and agreements.	PR.PT-P1: Removable media is protected and its use restricted according to policy.
	PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
	PR.PT-P3: Communications and control networks are protected.
	PR.PT-P4: Mechanisms (e.g. failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

Appendix B. Regulation Cross-Reference

The matrix consolidates the regulatory mappings of section 2.5. It is indicative only; the Privacy Office confirms applicability for each initiative and jurisdiction.

Table 20: PbD requirements across regulatory regimes

PbD requirement	GDPR (articles)	LGPD (articles)	CCPA/CPRA (Cal. Civ. Code)	HIPAA (45 CFR)
Purpose specification	5(1)(b), 13, 14	6 I (finality)	1798.100; 1798.110; 1798.115	164.502; 164.506; 164.508
Data minimization	5(1)(c), 25	6 III (necessity)	1798.100(c)	164.502(b); 164.514(d)
Accuracy	5(1)(d), 16	6 V (data quality)	1798.106	164.526
Lawfulness and fairness	5(1)(a), 6, 7, 9	7, 11; 6 IX (non-discrimination)	1798.120; 1798.125	164.506(b); 164.510
Purpose limitation	5(1)(b), 6(4)	6 II (adequacy)	1798.100(a), (c)	164.502(a); 164.508; 164.512
Storage limitation	5(1)(e)	15, 16	1798.100(a)(3)	164.530(j) (documentation retention)
Security	5(1)(f), 32–34	6 VII, VIII; 46–49	1798.100(e); 1798.150	164.306–164.312; 164.404–410
Transparency	5(1)(a), 12–14	6 VI; 9	1798.100; 1798.130; 1798.135	164.520
Intervenability	12–22	17–22	1798.105; 1798.106; 1798.110; 1798.120; 1798.121	164.522; 164.524; 164.526; 164.528
Accountability	5(2), 24, 28, 30, 35, 37–39	6 X; 37–41	1798.100(d); 1798.185	164.314; 164.504; 164.530
Prevention / by design	25	6 VIII (prevention); 46 §2	No express by-design duty	164.306 (security standards)

Appendix C. References

1. Cavoukian, A. (2009, rev. 2011). *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario.
2. International Conference of Data Protection and Privacy Commissioners (2010). *Resolution on Privacy by Design*. Jerusalem.
3. OECD (1980, rev. 2013). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.
4. World Privacy Forum (2006). *A Brief Introduction to Fair Information Practices*.
5. Regulation (EU) 2016/679, General Data Protection Regulation, in particular Articles 5, 25 and 32.
6. Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Brazil.
7. California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, Cal. Civ. Code §1798.100 et seq.
8. Health Insurance Portability and Accountability Act of 1996, Privacy and Security Rules, 45 CFR Parts 160 and 164.
9. NIST (2020). *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0*; and NIST Privacy Framework Version 1.1.
10. Hoepman, J.-H. (2014). *Privacy Design Strategies*. IFIP SEC 2014; and *Privacy Design Strategies (The Little Blue Book)*, Radboud University, 2020.
11. Colesky, M., Hoepman, J.-H. & Hillen, C. (2016). *A Critical Analysis of Privacy Design Strategies*. IEEE Security and Privacy Workshops.
12. Wright, D. (2026). *Privacy by Design (PbD) Position Paper*. Openthinka LLC.
13. Wright, D. (2026). *Enterprise Architecture M&A Integration Playbook*. Openthinka LLC.
14. Wright, D. (2026). *PII-Track: Enterprise PII Governance*. Openthinka LLC.