A Systematic Approach for the Protection of Personal Data and Privacy

Prudence Framework for GDPR and ISO/IEC 27701 Compliance

Miguel Azevedo, PhD
Runciter | Qity BV, Belgium
miguel@runciter.app | miguel@qity.be

2 August 2026 | Conceptual review, operational framework and reference implementation

ABSTRACT

The General Data Protection Regulation does not merely require organisations to possess privacy documents. It requires controllers and processors to implement appropriate measures, keep those measures effective as circumstances change, and be able to demonstrate what they have done. ISO/IEC 27701:2025 expresses the same operational problem as a privacy information management system: context, leadership, planning, support, operation, performance evaluation and improvement must work as a coherent system. For a young company, this can look disproportionate to its available resources. For an experienced data protection officer, the difficulty is different but related: facts, decisions, risks, controls, requests, incidents and evidence are distributed across people, spreadsheets, tickets, contracts and documents, making a current and defensible account of compliance unnecessarily hard to produce.

This paper proposes the Prudence Framework, a systematic method for implementing and demonstrating data-protection and privacy governance. Its central contribution is **accountability continuity**: every material conclusion about processing remains connected to the purpose, role, people, data, legal reasoning, risk, control, evidence, approval, review and subsequent change on which the conclusion depends. The framework represents the organisation, external entities, processing activities, affected groups, information resources, controlled documents, risks, technical and organisational measures, privacy actions and operational cases as distinct but related governed records. Life-cycle states, conditional requirements, workflow gates, statutory clocks, immutable histories, effectiveness evidence and review triggers act upon that structure.

The method is derived from a synthesis of the GDPR, authoritative European guidance, ISO/IEC 27701:2025 and adjacent privacy-risk and engineering literature. It is instantiated in Prudence, a working platform used here as a reference implementation. The paper shows how the structure supports records of processing, lawful-basis and role decisions, data-protection impact assessment, processor and transfer governance, data-subject requests, personal-data breaches, privacy risk treatment, statements of applicability, internal review and continual improvement. Two adoption patterns are considered: a small, data-intensive company establishing a defensible programme without building a large compliance department, and an experienced DPO replacing fragmented administration with controlled daily operations.

The framework does not make an organisation compliant, decide that processing is lawful, or turn software into a certifiable management system. Those conclusions remain the organisation's responsibility and depend on the truth of the information entered, the quality of decisions made and the effectiveness of measures in practice. Its purpose is narrower and more useful: to provide the information architecture, controlled workflows and evidence pathways through which an organisation can implement, operate, test and demonstrate its own GDPR and ISO/IEC 27701 programme.

Keywords: GDPR; ISO/IEC 27701; privacy information management system; accountability; privacy risk; data protection impact assessment; record of processing activities; data-subject rights; privacy engineering; compliance evidence; Prudence

I. INTRODUCTION

Personal-data compliance is often introduced as a list of deliverables: a privacy notice, a record of processing activities, processor clauses, a retention schedule, a data-protection impact assessment, and procedures for requests and incidents. All are potentially necessary. None, standing alone, demonstrates that the organisation knows what it does with personal data, has made the required decisions, operates the controls it describes, and revisits those decisions when the facts change.

The deeper obligation is accountability. Article 5(2) of Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR), makes the controller responsible for, and able to demonstrate, compliance with the processing principles. Article 24 requires appropriate technical and organisational measures that are reviewed and updated where necessary. Related duties distribute that expectation across data protection by design and by default, processor governance, security, breach response, impact assessment, records of processing and cooperation with supervisory authorities [1]. Before the GDPR, the Article 29 Working Party described accountability as an obligation to implement appropriate and effective measures and to demonstrate their effectiveness on request [2]. That distinction between possessing rules and operating a demonstrable control system remains decisive.

ISO/IEC 27701:2025 approaches the problem through a privacy information management system (PIMS). Unlike the 2019 edition, the 2025 edition is structured as a standalone management-system standard. Clauses 4 to 10 require the organisation to understand its context, establish leadership and policy, address risks and opportunities, support competent operation, control PIMS processes, evaluate performance and improve. Normative Annex A adds controls for PII controllers, PII processors and information-security considerations [6]. The standard therefore does not reduce privacy to a register or a collection of policies. It asks whether a governed system exists and whether that system works.

The practical difficulty is not a shortage of clauses, guidance or templates. It is the fragmentation between them. The purpose and lawful basis may be recorded in a processing inventory; affected persons and data categories in a data map; privacy information on a website; processor terms in a contract repository; transfer decisions in legal files; control evidence in security tools; requests in a ticketing system; and risk decisions in a spreadsheet. The DPO may understand the relationships, but the information system does not preserve them. When a processor changes a subprocessor, a product starts collecting a new field, a retention rule is revised or a data subject exercises a right, the organisation must reconstruct which decisions and controls are affected.

For a small contract research organisation, health-technology venture or fintech, fragmentation quickly becomes a governance risk. Such organisations may process sensitive, behavioural or financial information early in their development, while legal, security, product and quality responsibilities are concentrated in a small team. The founder can neither outsource accountability completely nor sustain an enterprise compliance estate. Proportionality is essential, but proportionality does not

mean informality. A small organisation still needs a reliable way to identify its material processing, make high-risk decisions, assign actions, preserve evidence and respond within statutory deadlines.

For an experienced DPO, the problem is less about knowing the law than about operating it at organisational scale. The European Data Protection Board's coordinated enforcement work on DPOs identified recurring concerns around resources, expert knowledge, conflicts and systematic involvement. It also emphasised the value of written reporting for accountability and traceability [5]. A DPO who spends time chasing record owners, reconciling inventories and rebuilding the history of decisions has less capacity to advise independently, monitor compliance and identify emerging risk.

These pressures have created a predictable market for privacy-management software. Yet software claims are often framed too broadly. GDPR compliance is not a product feature that can be activated, and conformity to ISO/IEC 27701 applies to an organisation's scoped PIMS, not to an application in isolation. Conversely, it is too weak to describe a specialist platform as merely a place to store templates. A well-designed platform can embody a substantive control architecture: a data model that reflects the regulated context, fields that capture decisions, state transitions that prevent premature closure, workflows that assign responsibility and time limits, links that preserve causality, gaps that expose incomplete obligations, and histories and exports that support assurance.

This paper asks what that architecture should contain. It proposes the Prudence Framework as a vendor-neutral method and uses the Prudence platform as its reference implementation. The framework is designed around five propositions.

First, privacy obligations are conditional. They depend on the organisation's role, purposes, categories of personal data and people, legal bases, jurisdictions, recipients, transfers, scale, technology, vulnerability, contractual allocation and risk. A system must represent those facts before it can determine which questions, decisions and evidence are relevant.

Secondly, processing activity is the principal operational anchor. It is not the only entity, and the framework does not force every fact into one record. It is the point at which purpose, lawful basis, data, affected people, sources, recipients, processors, transfers, retention, rights, security and impact normally converge.

Thirdly, documents are necessary but insufficient. A notice, legitimate-interests assessment, data-processing agreement or DPIA should remain a controlled document. Its status and conclusions should also be connected to the facts and workflows they govern. Otherwise a reviewer can find the file but cannot reliably determine whether it is current, applicable or effective.

Fourthly, risk must connect analysis to treatment and treatment to evidence. Consequences for individuals and consequences for the organisation are related but not interchangeable. Measures should be owned, implemented, tested and reviewed. Residual acceptance is a decision, not a number produced by a matrix.

Fifthly, demonstrability requires continuity over time. The system should record who decided what, against which baseline, with what evidence, subject to which conditions, and which later event requires review. This paper calls that property **accountability continuity**.

The result is intended to support two readers without becoming two papers. Founders and executives should be able to see what a proportionate, defensible privacy programme entails and where management decisions remain necessary. DPOs should be able to evaluate whether the proposed records, relationships, workflows and controls are adequate for daily professional work. Both should be able to distinguish a platform capability from an organisational outcome.

II. METHOD AND SCOPE

This work is a conceptual standards synthesis, structured narrative review and implementation description. It is not legal advice, a certification interpretation, an empirical validation study or an assertion that use of a named product establishes conformity. The method began with the operational question: what must an organisation be able to know, decide, do, test and retrieve if it is to implement and demonstrate data-protection and privacy governance?

Four source groups were examined. The first comprised the GDPR and authoritative European guidance on accountability, data protection by design and by default, controller and processor roles, DPIA, rights and personal-data breaches [1-5,28-31]. The second comprised ISO/IEC 27701:2025 and related privacy, impact-assessment and risk instruments, particularly ISO/IEC 29100, ISO/IEC 29134, ISO/IEC 27557 and the NIST Privacy Framework [6-10]. The third comprised privacy-engineering research on translating principles into designs, connecting law and engineering, and making privacy requirements usable in system development [13-22,27,35]. The fourth comprised implementation and organisational studies addressing adoption barriers, success factors, fragmented practices and small-organisation experience [17-26].

Sources were selected for functional relevance rather than bibliometric completeness. A source was treated as central where it helped answer at least one of six questions: how accountability should be evidenced; how processing context should be represented; how risk to individuals should be assessed; how legal and technical decisions should be connected; how operational obligations should be controlled; and how a management system should monitor and improve its own effectiveness. The search was updated through 2 August 2026. Because this was a structured narrative review, no claim of exhaustive retrieval is made.

The framework was then instantiated against the documented data model and workflows of Prudence. The prototype was examined at three levels. First, the record model was tested for its ability to represent organisation and role context, processing, affected persons, information resources, external parties, documents, transfers, consent, risk, controls and operational cases. Secondly, workflows were tested for ownership, mandatory and conditional fields, life-cycle state, approval, statutory timing, gaps, actions, evidence and review. Thirdly, outputs were examined for their ability to support records of processing, registers, management review and external assurance [39-41].

The assessment principle was capability, not customer outcome: **can the platform's data model, required or conditional fields, relationships, lifecycle gates, workflows, evidence and exports represent and demonstrate the requirement when used correctly?** A capability was considered native where the platform provides a dedicated governed record or workflow. It was considered template-supported where a controlled document can validly satisfy the requirement and the platform can version, approve, link, review and evidence that document. It was considered integration-dependent where the authoritative control or evidence properly belongs in another system, such as identity management, secure development, human resources, finance, product configuration or physical security. It was considered organisational where no software can make the substantive decision or perform the real-world action.

This allocation avoids two errors. The first is to mark a requirement as absent merely because it is not implemented as a separate screen. For example, responsibility may be demonstrated through mandatory owners across controlled records, a governance document and approval histories rather than through a module called “responsibility”. The second is to mark a requirement as complete because a field or template exists. A lawful basis selected without valid reasoning, a processor record unsupported by due diligence, or a measure without implementation and effectiveness evidence remains weak in practice.

The current ISO analysis uses ISO/IEC 27701:2025, as adopted in the searchable ABNT NBR ISO/IEC 27701:2026 edition supplied for this work. Clause and control summaries are interpretive paraphrases. They do not reproduce the standard and should be verified against a licensed copy during formal PIMS design or certification preparation.

The reference implementation was subjected to five scenario tests:

1. whether a reviewer could start with an operational processing activity and reconstruct its purpose, role, lawful basis, affected groups, data, recipients, transfers, retention, relevant documents, risks, measures, approvals and review status;
2. whether high-risk processing could be used as the factual starting point for a DPIA, while a missing or unpublished DPIA remained a visible gap rather than being hidden by inventory status;
3. whether a data-subject request or breach could be governed as a case with identity, scope, decisions, evidence, responsibility and statutory time;
4. whether a privacy risk could preserve separate consequences for data subjects and the organisation and connect treatment to technical and organisational measures, actions, effectiveness evidence and residual approval; and
5. whether a material change could identify the records, decisions, documents, controls and reviews that may no longer be valid.

These tests establish internal coherence and implementation feasibility. They do not establish that every deployment will be correctly configured, that organisational controls operate, or that a supervisory authority or certification body will accept a particular conclusion.

III. WHY PRIVACY COMPLIANCE RESISTS CHECKLIST TREATMENT

3.1 A conditional system of obligations

The GDPR combines universal principles with context-dependent duties. Lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, security and accountability apply broadly, but their implementation depends on the processing. The information given to an employee is not the same as the information given to a clinical-trial participant. Legitimate interest requires a different analysis from consent. A processor has different decision authority from a controller. A transfer to a third country introduces questions that do not arise for a recipient within the same protected legal environment. DPIA is required because of likely high risk, not because an organisation has reached a particular size [1].

Conditionality has an information-design consequence. The system cannot reliably ask only "Do we have a DPIA policy?" It must be able to ask "Which processing activities meet the organisation's screening criteria, which have been assessed, what was the decision, what treatment is open, who accepted residual risk, and which change requires the assessment to be reviewed?" The first question produces a document. The second produces accountable operation.

The same applies to rights. A generic procedure may define the approach to access, rectification, erasure, restriction, objection and portability, but each request still requires an operational record. The organisation must identify the requester, interpret scope, find relevant data and systems, consider exceptions, coordinate recipients where required, provide an intelligible response and preserve evidence within the applicable time. The EDPB's guidance on access demonstrates how quickly a simple legal right becomes a multi-step operational process [30].

3.2 A document can state a control without proving it operates

Policies and assessments are important because they formalise expectations and reasoning. Their evidential weakness arises when they are detached from implementation. A retention policy can say that candidate data is deleted after twelve months while a recruitment platform retains it indefinitely. A DPIA can approve a service subject to pseudonymisation while the production configuration still exposes direct identifiers. A processor agreement can contain Article 28 terms while the service owner enables an unassessed subprocessor. In each case the document exists, but the asserted control and operational fact have diverged.

Privacy engineering research has repeatedly examined the translation gap between legal principles and technical design. Spiekermann and Cranor distinguish policy-oriented privacy management from engineering choices embedded in systems [13]. Hoepman's strategies provide ways to move from abstract privacy goals towards architectural action [14]. Gürses and del Álamo describe privacy engineering as an emerging field that must negotiate legal, organisational and technical meanings [15]. Studies of practitioners report difficulty allocating responsibility and authority, particularly where engineers are expected to realise legal concepts without an operational bridge [17,18].

A controlled platform cannot eliminate that difficulty, but it can make the bridge explicit. A legal conclusion becomes a governed decision. The decision identifies which processing it applies to. Measures become owned control records rather than prose. Implementation and effectiveness evidence are linked without pretending that a privacy platform is the authoritative source for every technical fact. Review triggers expose when the decision should be revisited.

3.3 Fragmentation breaks causality

Fragmented compliance administration creates more than inefficiency. It obscures causality. Consider a fintech that adds account-aggregation data from a new provider. The change may affect the processing purpose, categories, source, contract, processor allocation, transfer position, privacy notice, retention logic, information-security controls, DPIA, legitimate-interests analysis, data-subject request search scope and breach impact. If each artefact is separately owned and no relationship expresses why it is connected, the change depends on memory and coordination rather than on the control system.

Requirements-engineering and implementation studies describe analogous problems. GDPR requirements are broad, interacting and difficult to translate into technical specifications [19-22,26]. Model-based and process-oriented proposals improve traceability by giving requirements and processing facts explicit structure [22,27]. Research in small organisations shows that practical methods must fit limited expertise and resources while still integrating legal, organisational and technical work [23]. Broader reviews identify information governance, enterprise architecture and cross-functional coordination as enablers, and warn that standards used without an implementation path can leave an operational gap [24].

The design implication is that a privacy platform should preserve semantic relationships, not just hyperlinks. "Processing Activity uses Processor" has a control consequence. "DPIA assesses Processing Activity" has another. "Risk affects Data Subject Set", "TOM treats Risk", "Action implements TOM" and "Evidence demonstrates effectiveness" create a navigable causal chain. A generic "related documents" folder does not.

3.4 Accountability is temporal

Compliance conclusions decay. The lawful basis may remain stable while the purpose expands. A processor may change its location or subprocessors. A security measure may be implemented but later fail testing. A data-subject group may become more vulnerable. An initially low-risk activity may reach scale. A regulator or court may clarify the applicable law. The organisation must therefore preserve both the current position and the history of how it arrived there.

Article 24 expressly anticipates review and updating. Article 25 requires measures to be selected with regard to state of the art, cost, nature, scope, context, purposes and risk, all of which can change [1,3]. ISO/IEC 27701 reinforces the point through performance evaluation, internal audit, management review, corrective action and continual improvement [6]. Accountability is therefore not a snapshot. It is the controlled ability to explain the current state, the earlier state and the

reason for transition.

3.5 The scaling problem is real, but informality is not the answer

The European Commission's second report on the application of the GDPR concluded that the Regulation had delivered important results while identifying the need for clearer, more actionable support, particularly for SMEs, small operators and research organisations [4]. EDPB guidance and SME resources attempt to make obligations more accessible [33]. That support is valuable, but a small organisation still has to convert guidance into its own facts, decisions and evidence.

The appropriate response is proportionality. The number and depth of records should follow the organisation's roles, processing and risk. A five-person software company with one business-to-business product does not need the same governance estate as a multinational clinical research network. It may nevertheless need a complete account of its few material processing activities, a defensible processor and transfer position, one well-run DPIA, a working request and breach process, and evidence that important measures operate. A systematic architecture allows this selectivity because it shows which obligations are triggered and where gaps remain. A checklist often produces the opposite outcome: many generic documents and too little control over the processing that matters most.

IV. NORMATIVE AND RESEARCH FOUNDATIONS

4.1 GDPR accountability as an operating requirement

The GDPR's architecture supports a systems interpretation. Article 5 sets the principles and makes accountability explicit. Article 24 requires the controller to implement, review and update appropriate measures. Article 25 places data protection into design and default settings. Articles 28 and 29 govern processing by others and under authority. Article 30 requires records of processing. Articles 32 to 36 connect security, breach response, risk, DPIA and prior consultation. Articles 12 to 22 define rights that the organisation must be able to execute, not merely acknowledge [1].

The Article 29 Working Party's accountability opinion proposed programmes scaled to the organisation and processing, with mapped operations, allocated responsibility, procedures for rights and breaches, impact assessment, training, monitoring and verification [2]. EDPB guidance on Article 25 likewise treats effectiveness as material. Measures must actually implement the principles and protect rights, and controllers must be able to demonstrate that the chosen measures are effective [3]. The emphasis is consistent: context, action, effectiveness and evidence.

This paper does not treat every GDPR article as a software requirement. Some provisions concern supervisory authorities, remedies, jurisdiction or legislative powers. Some obligations can be represented in a platform but performed only by people or connected systems. The relevant point is that the controller or processor should be able to locate the processing context, decision, responsible person, measure and evidence necessary to support its position.

4.2 ISO/IEC 27701:2025 as the management-system layer

ISO/IEC 27701:2025 provides a coherent organisational cycle. Clause 4 establishes the organisation and PIMS context, relevant interested parties, scope and processes. Clause 5 requires leadership, policy, assignment and communication of roles. Clause 6 covers risks and opportunities, privacy risk assessment and treatment, objectives and planning of changes. Clause 7 addresses resources, competence, awareness, communication and documented information. Clause 8 moves from planning to operational control, including performance of privacy risk assessment and treatment. Clause 9 requires monitoring, measurement, analysis, evaluation, internal audit and management review. Clause 10 addresses nonconformity, corrective action and continual improvement [6].

Normative Annex A adds controls differentiated by role. Controller controls address matters such as purpose and lawful basis, consent, processing records, obligations to PII principals, data protection by design and default, sharing, transfers and disclosure. Processor controls address customer instructions, processing terms, assistance, records, transfer and disclosure, return or disposal, and related operational duties. Security considerations connect privacy requirements to an adequate information-security programme. The standard also requires a statement of applicability in the risk-treatment process, including selected controls, justification, implementation status and reasons for exclusions [6].

Two features are especially important for the framework. First, privacy risk assessment considers consequences for PII principals as well as consequences for the organisation. This resists the common practice of evaluating privacy only through financial, regulatory or reputational exposure. Secondly, management-system clauses prevent the control catalogue from becoming static. Scope, objectives, resources, competence, internal audit, management review, corrective action and change are part of conformity.

4.3 Supporting privacy-risk and engineering instruments

ISO/IEC 29100 supplies a privacy framework and shared vocabulary; ISO/IEC 29134 structures privacy impact assessment; ISO/IEC 27557 addresses organisational privacy risk and distinguishes impacts on individuals from organisational consequences [7-9]. The NIST Privacy Framework similarly treats privacy through enterprise risk management and is deliberately usable across organisation size, sector and jurisdiction [10]. ENISA guidance examines privacy and data-protection engineering as the selection and implementation of concrete controls, not the repetition of principles [11,12].

These sources converge on an important design point: privacy impact is not identical to organisational compliance exposure. An activity can cause meaningful loss of autonomy, discrimination, exclusion, chilling effects or other consequences for people even if the organisation expects limited financial loss. Conversely, an administrative violation may create substantial organisational exposure without the same degree of individual harm. The assessment should retain both views and allow governance to respond to each.

Academic privacy-engineering work supplies methods for moving from principles to system design, but also demonstrates why a method needs organisational support. Privacy strategies, patterns, threat modelling, requirements models and process modelling can produce better designs [13-16,19,22,27,35]. Their use depends on defined responsibility, appropriate expertise, access to processing facts and integration with development and business decisions [17,18,21,23-26]. The Prudence Framework therefore treats engineering techniques as possible risk treatments or design evidence inside a wider management and accountability system.

4.4 The implementation gap the framework addresses

The evidence does not show that organisations lack frameworks. It shows that they struggle to turn multiple frameworks into one operating arrangement. The GDPR supplies legal duties. ISO/IEC 27701 supplies a management system and control set. Privacy engineering supplies design methods. Risk instruments supply assessment approaches. The missing layer is often the controlled connection among factual processing, decisions, implementation, operational events and assurance.

That connection cannot be solved by a universal compliance score. A numerical score can assist prioritisation, but it can also collapse unlike conditions and obscure judgement. An overdue access request, a missing transfer mechanism, a failed encryption test and an unsigned policy are not interchangeable points. The framework therefore derives programme health from named records and conditions. Every red indicator should be traceable to the fact, owner, required action and evidence needed to close it.

Table 1: From checklist administration to controlled privacy operation

Compliance problem	Checklist or document-only response	Controlled-system response	Defensible evidence
A new purpose is added to an existing service	Update a policy at the next review	Change the Processing Activity, route legal and privacy review, identify affected notices, risks, recipients and controls	Version history, decision, approver, linked revisions and completed actions
A high-risk activity is already operating but no DPIA is published	Hide the activity in draft or record "DPIA pending" in notes	Record operational reality, raise an explicit blocking or escalated gap, derive the DPIA from the activity and assign treatment	Activity baseline, screening rationale, gap age, DPIA decision and treatment evidence
A data subject exercises access	Refer staff to a rights policy	Open a governed request case, verify identity, define scope, search linked systems and processors, record exceptions, respond and preserve evidence	Statutory clock, actions, correspondence, response package, decision history
A privacy control is described as implemented	Mark the policy complete	Link the control to affected risks and processing, require an owner, implementation evidence, effectiveness test and review date	Technical or organisational evidence, test result, reviewer and residual decision
A processor changes a subprocessor	Save the notice in the vendor folder	Change the external-entity record, assess instruction, location, transfer, due diligence, contract and affected activities	Approval record, updated contract and transfer assessment, affected-processing report
Management asks whether the programme is healthy	Count completed documents	Derive health from overdue cases, unresolved gaps, stale reviews, missing evidence, accepted risk and failed controls	Reproducible dashboard backed by named records and drill-down history

Table 2: Contribution and boundary of selected instruments

Instrument	Principal contribution	Use in the Prudence Framework	Boundary
GDPR [1]	Binding principles, rights and controller/processor obligations	Determines legal outcomes, triggered workflows, evidence and deadlines	Does not prescribe a specific software architecture or management-system form
ISO/IEC 27701:2025 [6]	Standalone PIMS requirements and controller, processor and security controls	Provides management-system cycle, risk treatment, SoA, audit, review and improvement structure	Conformity belongs to the scoped organisational PIMS, not the platform alone
ISO/IEC 29100:2024 [7]	Privacy vocabulary and high-level principles	Normalises concepts and principle coverage	Does not itself establish operational workflow or certification requirements
ISO/IEC 29134:2023 [9]	Guidance for privacy impact assessment	Informs DPIA stages, consultation, treatment, reporting and review	GDPR thresholds and legal conclusions remain controlling where applicable
ISO/IEC 27557:2022 [8]	Organisational privacy-risk management	Supports dual analysis of impact on people and consequences for the organisation	Risk method must be tailored and integrated with the PIMS
NIST Privacy Framework 1.0 [10]	Flexible privacy-risk outcomes through enterprise risk management	Supports profiling, communication and cross-functional risk thinking	Voluntary and law-agnostic; not a certificate of legal compliance
EDPB guidance [3,28-31]	Authoritative interpretation of operational GDPR duties	Informs decision criteria, workflow content and evidence expectations	Application remains fact- and jurisdiction-dependent
Privacy-engineering literature [13-22,27,35]	Strategies, models and experience translating privacy into design	Supplies design and assurance methods that can be linked as treatments and evidence	No single method covers organisational accountability or every legal duty

V. THE PRUDENCE FRAMEWORK

5.1 Accountability continuity

The central design property of the Prudence Framework is accountability continuity. A conclusion is accountable when its subject, decision-maker, factual baseline, reasoning, evidence, conditions and effective state can be reconstructed. It has continuity when later information can be routed back to the conclusions it may invalidate.

Consider the statement "this processing is lawful on the basis of legitimate interests". In a document-only implementation, that sentence may appear in an assessment. Under the framework, the conclusion identifies the controller, specific purpose, necessity reasoning, interests pursued, affected data-subject set, reasonable expectations, possible impacts, safeguards, privacy information, responsible owner, reviewer, approval date and planned review. It is linked to the Processing Activity and to any risks, TOMs or actions that make the balance acceptable. A new purpose, more intrusive data, a vulnerable group, an upheld objection, a complaint or a failed safeguard can then trigger review of that particular conclusion.

Continuity does not imply that every change automatically invalidates every approval. It supplies a controlled route for impact analysis. The reviewer can determine that the conclusion remains valid, requires conditions, needs revision, or no longer supports the processing. Without the relationship, the organisation may never ask.

5.2 Six interacting layers

The framework separates six layers so that different kinds of control are not conflated.

1. **Context.** Organisation, jurisdictions, controller or processor role, interested parties, external entities, business units, data-subject sets, purposes, information resources and PIMS scope establish which obligations and perspectives apply.
2. **Controlled records and decisions.** Processing Activities, documents, consents, transfers, agreements, assessments and approvals preserve the governed position.
3. **Operational workflows.** Requests, breaches, processor engagement, consultations, actions, audits and reviews turn policy into assigned and time-bound work.
4. **Risk and control.** Privacy Risks, DPIAs, technical and organisational measures and treatment actions connect consequences to implementation and residual decisions.
5. **Evidence and assurance.** Attachments, references to authoritative systems, effectiveness results, histories, exports and reports support verification.
6. **PIMS management.** Policy, objectives, competence, communication, statement of applicability, internal audit, management review, nonconformity, corrective action and improvement govern the whole system.

The layers are not maturity levels. Even a small programme needs some element of each. Proportionality determines depth and volume. A start-up may have one PIMS objective, a compact policy set and a small number of Processing Activities, but it still needs reliable rights and breach workflows, risk decisions and management review.

5.3 Governed records rather than free-form forms

A governed record has a stable identity, type, owner, state, required and conditional information, relationships, history and defined route to closure or the next decision. Free-form narrative remains available where judgement requires it, but narrative is not used as a substitute for information that must be filtered, compared, triggered or reported.

This design is particularly important for requiredness. A blanket collection of every possible field makes the platform burdensome and encourages superficial completion. A minimal form that never changes misses legal conditions. The framework uses destination-state and context-sensitive requirements. Information needed to save an early draft can be limited. Information required to move a Processing Activity into legal review, approval or operational use should reflect its role, lawful basis, special-category data, children or vulnerable people, transfers, automated decisions, scale and risk.

Life-cycle state must express governance meaning. "Draft" means the record is being assembled. "Legal review" or "Privacy review" means a named reviewer is considering the relevant decision. "Approved" means the stated configuration and conditions have been authorised by the responsible role. "In use" records that processing is operational. It is not, by itself, a legal authorisation. "Suspended" and "Retired" distinguish temporary restriction from the end of authorised processing and trigger retention or deletion actions where applicable.

This distinction resolves a recurrent DPIA problem. An organisation may discover an activity that is already taking place and likely requires a DPIA. Refusing to record it as "In use" makes the inventory inaccurate. Allowing "In use" without consequence makes the governance weak. The framework records the operational fact, creates a visible and owned gap, allows a DPIA to be derived from the current processing baseline, and routes the matter for escalation. The missing DPIA remains observable until an authorised decision is published. The label describes reality; it does not legitimise it.

5.4 Gaps as first-class control information

A gap is not a generic warning or a missing-field count. It states the unsatisfied condition, why it matters, which record and state it affects, what remedy is expected, who owns the remedy, when it is due and what evidence will permit closure. Some gaps prevent a state transition. Others permit the system to reflect current reality while escalating an unauthorised, overdue or higher-risk condition.

Examples include a Processing Activity without an assigned owner, special-category processing without an Article 9 condition, a processor without approved terms, a transfer without a recorded mechanism, high-risk processing without a published DPIA decision, an overdue DSR, a breach notification decision approaching 72 hours, a TOM without effectiveness evidence, and a management review action past its due date. Because each gap is attached to a governed record, a programme dashboard can aggregate them without creating a separate and unverifiable compliance score.

VI. CONTROLLED ENTITY AND RELATIONSHIP MODEL

6.1 The organisation and responsible actors

The framework begins with the organisation because legal role and management-system scope are organisational facts. The Organisation record should identify legal identity, establishments, jurisdictions, business units, controller and processor contexts, representative and DPO arrangements, supervisory-authority context, PIMS scope, policy ownership and senior-management accountability. People and roles should be reusable objects so that ownership is not reduced to names written in documents.

Assigned ownership performs several functions. It identifies who must keep a Processing Activity current, who coordinates a request, who owns a Risk, who implements a measure, who approves residual risk and who provides evidence at review. Responsibility therefore appears both in governance documents and on the operational records through which the responsibility is exercised. This answers the common concern that "organisation and responsibilities" are only template content. A controlled template establishes the governance arrangement; record ownership and approval history demonstrate its operation.

6.2 External entities and role allocation

An Entity represents another organisation or relevant party: customer, processor, subprocessor, joint controller, independent controller, recipient, data source, consultant, authority or other participant. It should preserve legal identity, locations, contact and DPO details, service rela-

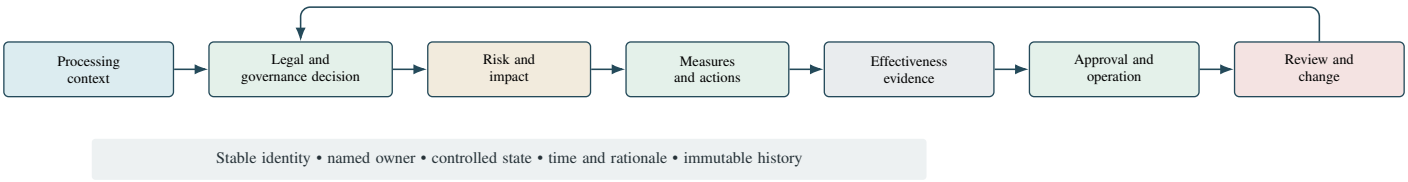

Figure 1: Accountability continuity connects processing context to decisions, risk, controls, evidence and operation. Later evidence is routed back to the conclusions whose assumptions it may change.

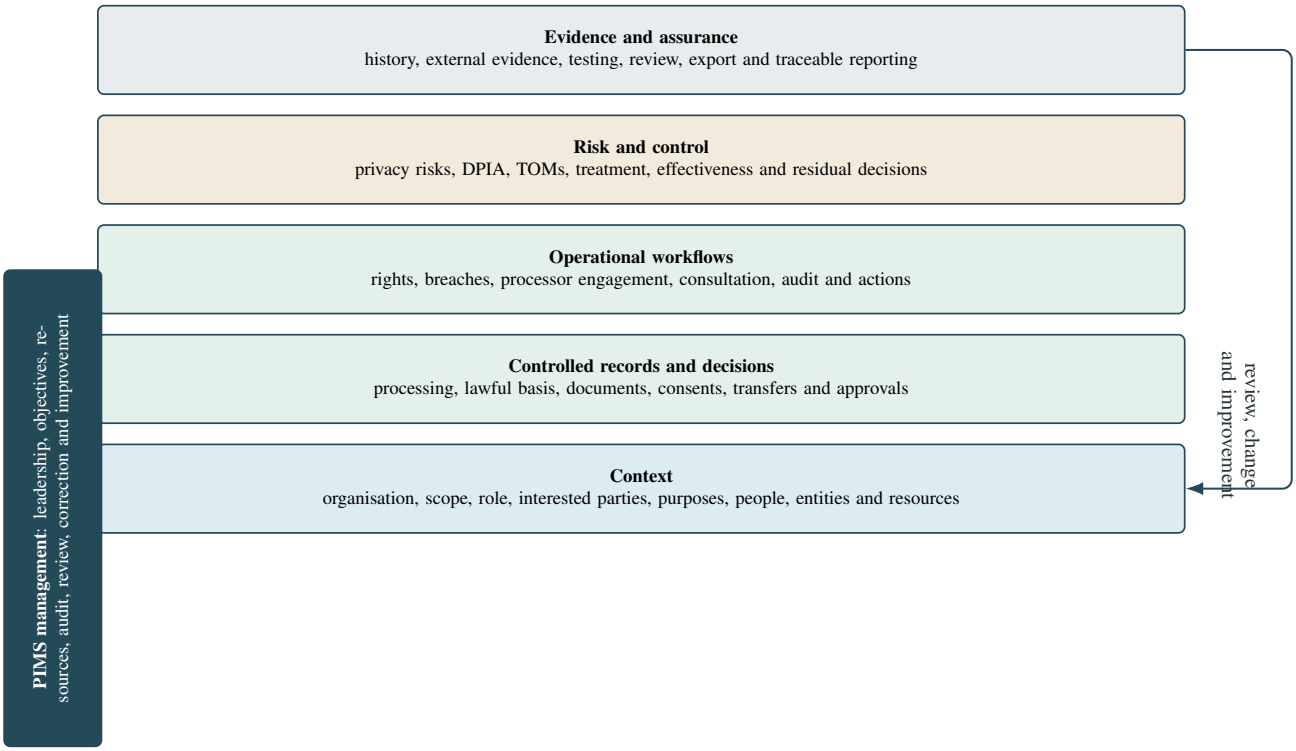

Figure 2: The Prudence Framework separates five operational layers while PIMS management governs all of them through leadership, objectives, assurance and improvement.

tionship, privacy role, contractual status, due diligence, subprocessors, transfer relevance, linked Processing Activities and review state.

Role cannot be inferred reliably from a contract label. EDPB guidance emphasises the factual allocation of purposes and essential means [28]. The platform can structure the analysis and preserve the decision, but the organisation must determine the role correctly. A single supplier may also act in different capacities for different activities. The relationship between Entity and Processing Activity should therefore carry context rather than forcing one universal label on the supplier.

6.3 Processing Activity as the operational anchor

The Processing Activity is the central contextual record. At minimum, it should identify reference, name, business purpose, controller or processor role, owner, lifecycle state, relevant entities, categories of people and personal data, sources, recipients, systems or information resources, retention, security measures, transfers, lawful basis and special-category condition where applicable. Conditional fields should address consent, legitimate interests, legal obligation, public task, children, automated decision-making, monitoring, large scale, innovative technology and other factors material to risk and transparency.

The Processing Activity should not duplicate every linked document or operational case. It anchors them. A privacy notice explains the processing to people. A legitimate-interests assessment preserves balancing. A transfer impact assessment deals with a particular transfer context. A DPIA records the high-risk assessment and decision. A processor agreement establishes terms. The Processing Activity allows a reviewer to determine which of those records apply and whether they are current.

The resulting record of processing is a projection of governed facts, not a parallel spreadsheet. Article 30 requires specified information, but the internal record may contain more to support accountability. The framework therefore distinguishes the complete operational record from the formal controller or processor RoPA export. An export can be generated in the required form without discarding the relationships and evidence needed to govern it.

6.4 Data-subject sets and information resources

A data-subject category in a RoPA is often too broad for impact analysis. The framework uses a Data Subject Set to represent the people affected in a particular context, including children, patients, employees, applicants, borrowers, investigators, customers, users, bystanders or vulnerable groups. The record can preserve scale, geography, relationship with the organisation, dependency, power imbalance, reasonable expectations, accessibility or communication needs and potential consequence domains.

Information Resources identify the applications, databases, services, physical stores, interfaces or other locations in which personal data is collected, used, transmitted or retained. A Resource record should identify ownership, provider, hosting, location, sensitivity, access and security context, retention or deletion capability, incident route and linked processing. It need not replace a configuration-management database, cloud inventory or security tool. Its function is to identify privacy-relevant systems and point to the authoritative evidence.

Together, Data Subject Sets and Resources make rights, breach and risk work more reliable. A request can identify which resources may hold the requester's data. A breach can identify affected processing

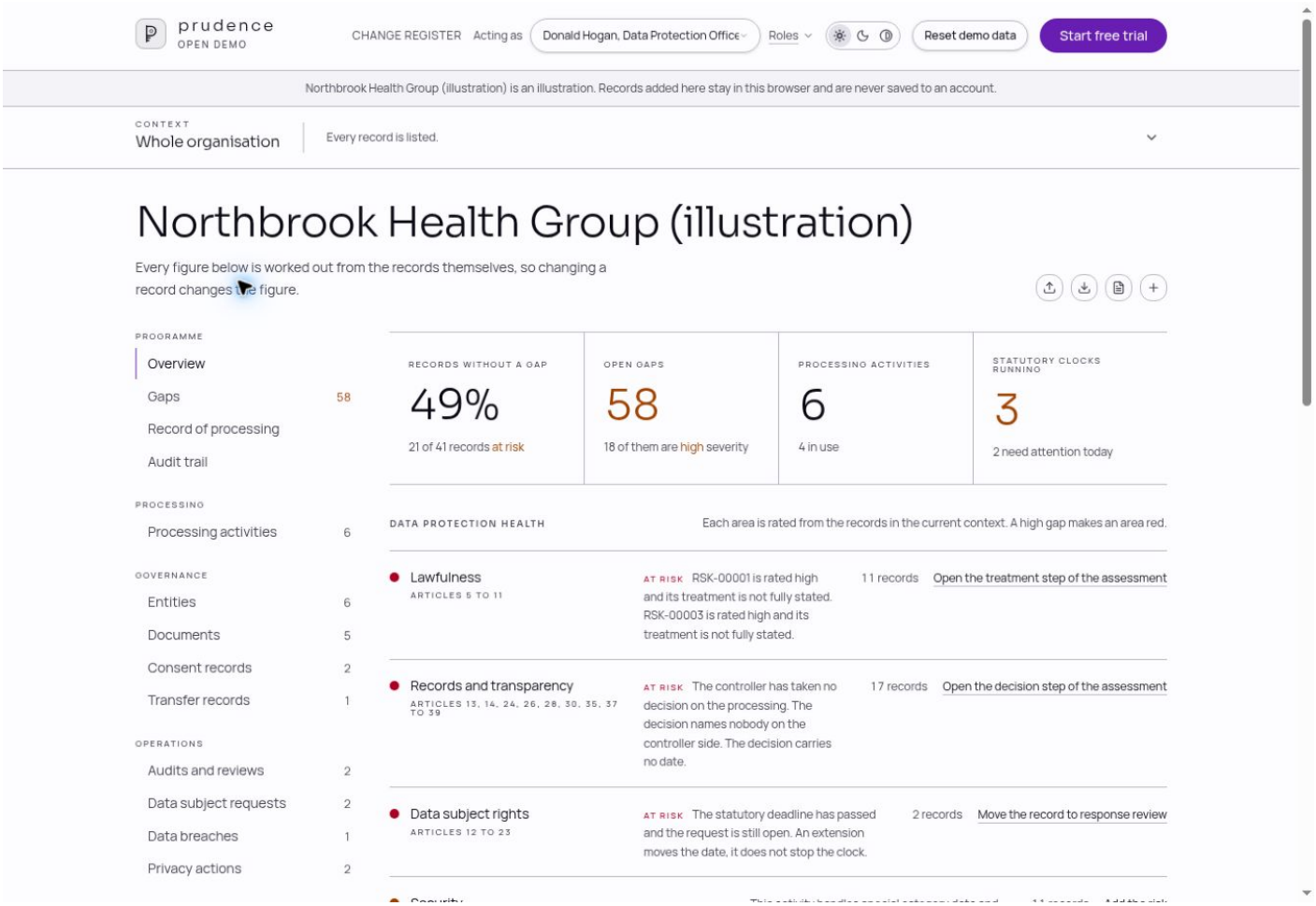

Figure 3: Illustrative Prudence programme view. Health indicators are derived from named records, gaps, statutory clocks and review conditions. The dashboard is a navigation and prioritisation surface; it is not a legal-conformity score.

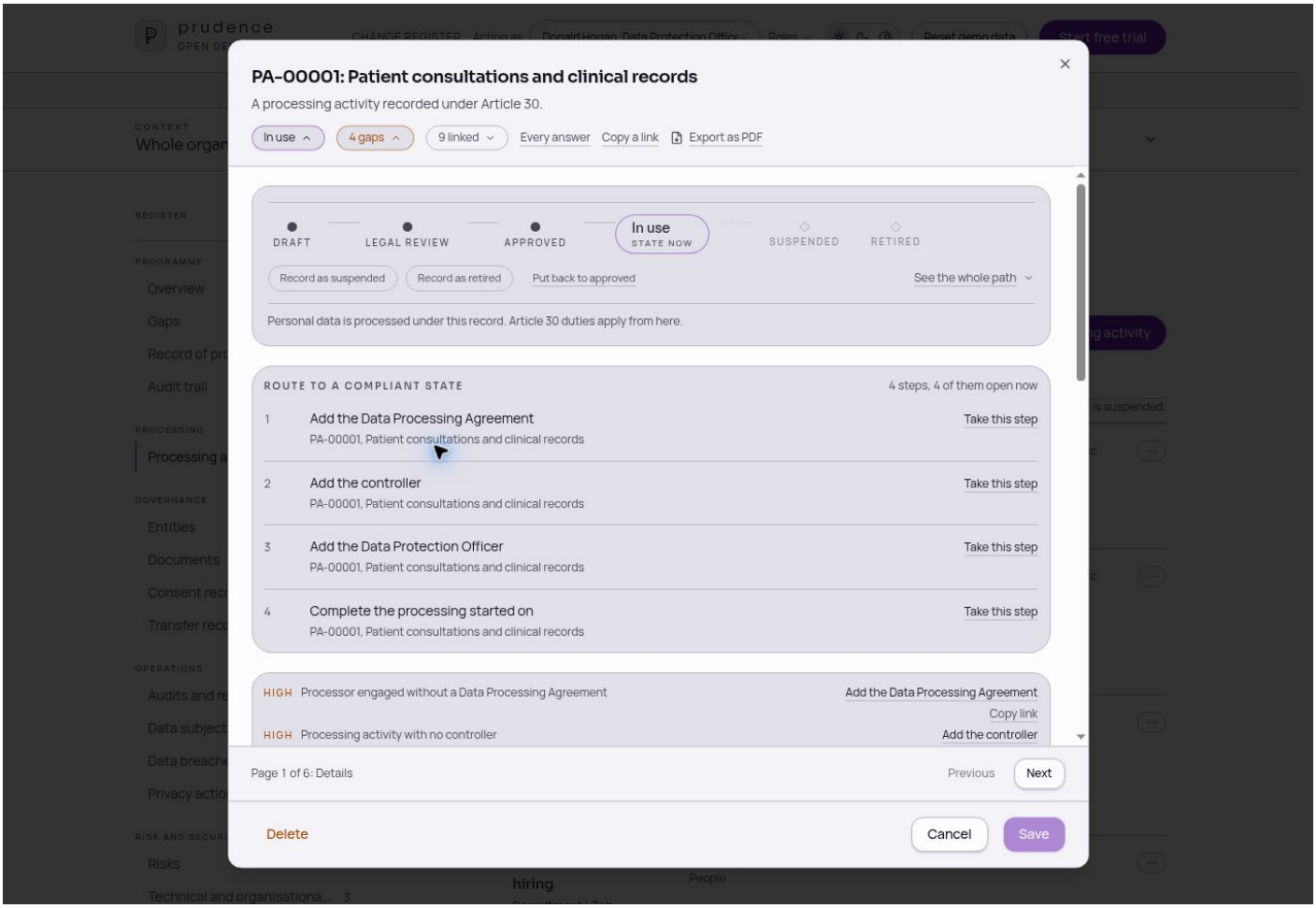

Figure 4: Illustrative in-use Processing Activity. The lifecycle rail records operational state; route-to-state logic identifies missing decisions and evidence. 'In use' records present fact and does not, by itself, authorise the processing.

and groups. A DPIA can analyse consequences for actual people rather than an abstract "data subject". A retention change can find the systems expected to implement it.

6.5 Controlled documents and operational records

The Document record covers privacy notices, policies, agreements, legitimate-interests assessments, DPIAs, transfer assessments, consent language, procedures, audit reports, management-review outputs and other controlled content. Core properties include type, owner, approver, version, status, effective date, review date, scope, supersession and links to the records it governs.

Operational records cover events that have their own timing and decisions: data-subject requests, personal-data breaches, privacy actions, audits, reviews, consents and transfers. They are not attachments to a policy because each instance must be assigned, processed and evidenced. A policy explains how the organisation responds to a request. The DSR record demonstrates what it did for one person.

6.6 Semantic relationships and impact analysis

Relationship names should express control meaning. "Processing Activity involves Entity as processor" is different from "Processing Activity discloses personal data to Entity as independent controller". "Risk affects Data Subject Set" is different from "Risk threatens organisational objective". "TOM treats Risk" is different from "Evidence verifies TOM". These distinctions allow conditional questions and impact queries.

The principal topology is centred on Processing Activity but remains many-to-many. One Resource can support several activities. One activity can use several Resources. A privacy notice can govern several activities; an activity can require several notices. A TOM can treat multiple risks, and a risk can require multiple TOMs. A processor can serve different roles in different contexts. The relationship should therefore be a controlled association where it carries material properties such as role, purpose, instruction, applicability, effective date or evidence.

VII. RISK, CONTROLS, DPIA AND EVIDENCE

7.1 A dual perspective on privacy risk

Privacy risk is frequently assessed as risk to the organisation: regulatory sanction, litigation, operational interruption or reputational damage. Those consequences matter to management, but they are not a substitute for effects on people. The GDPR's risk-based provisions focus on the rights and freedoms of natural persons. ISO/IEC 27701:2025 and ISO/IEC 27557 also preserve the distinction between consequences for PII principals and consequences for the organisation [1,6,8].

The framework therefore records one likelihood assessment against separately described and rated consequence perspectives. It does not average the two into a single apparently precise value. The Risk record identifies source, event or condition; affected Processing Activities, Data Subject Sets, Resources and obligations; existing measures; likelihood rationale; consequences for people; consequences for the organisation; inherent position; treatment; residual position; owner; reviewer; approver; and review triggers.

Consequences for people can include physical, material and non-material effects: loss of confidentiality, identity abuse, financial loss, discrimination, exclusion, loss of opportunity, exposure of sensitive circumstances, inability to exercise rights, chilling effects, loss of autonomy or control, distress and safety consequences. Organisational consequences can include regulatory action, contractual breach, remediation cost, disruption, lost trust and strategic limitation. The language should remain scenario-specific rather than becoming a catalogue selected without reasoning.

Risk criteria should define how likelihood and consequence are evaluated, when treatment is mandatory, who may accept residual positions and what requires escalation. A matrix can support consistent visualisation, but it cannot decide acceptability. The decision record should explain why the residual position is accepted, under which conditions, by whom and until when.

7.2 Technical and organisational measures as governed controls

A TOM should be more than a checkbox such as "encryption" or "training". The record should state its objective, design, scope, owner, implementation state, affected processing and risks, evidence source, test method, result, reviewer, review interval and failure route. Where the authoritative evidence belongs in another system, the TOM should reference it and record the privacy conclusion without copying volatile technical detail into the PIMS.

For example, a TOM may require role-based access to a clinical data environment. Identity-management configuration and access logs remain in the security system. Prudence records where the control applies, who owns it, which Risks it treats, the expected control outcome, the evidence reference, the latest effectiveness conclusion and the next review. A failed access review can then create an Action, revise residual risk and trigger DPIA review where material.

The distinction between design, implementation and effectiveness is important. A control can be well designed but not deployed. It can be deployed but inconsistently operated. It can operate as specified but fail to reduce the relevant risk. Evidence should be evaluated against the intended outcome, not merely attached.

7.3 DPIA as a decision workflow derived from processing

Article 35 requires a DPIA before processing likely to result in high risk. It also requires review where necessary, at least when the risk represented by processing changes [1]. DPIA is therefore neither a generic privacy questionnaire nor a static report. It is a controlled analysis and decision process.

The framework uses six stages: scope, risk analysis, treatment, consultation, decision and baseline. Scope is inherited from linked Processing Activities so that purpose, people, data, resources, recipients, transfers and current controls do not have to be recreated manually. Screening records why DPIA is or is not required. Risks and treatments use the same governed Risk, TOM and Action records as the wider programme. Consultation records DPO advice and, where appropriate, the views of data subjects or their representatives. Decision records approval, conditions, residual high risk, prior-consultation position and responsible authority. The published baseline identifies the assessed configuration and review triggers.

This pattern deliberately permits an existing Processing Activity to be recorded as in use while a DPIA is still missing or unpublished. That behaviour supports accurate inventory and pragmatic remediation. It is defensible only because the framework makes the condition explicit: the DPIA gap is flagged, owned, dated and escalated; the platform does not describe "In use" as lawful or approved; and the organisation must decide whether to restrict or suspend actual processing while the assessment is completed. Where high-risk processing is proposed rather than discovered, the governance route should hold authorisation until the required DPIA decision exists.

Once a baseline is published, changes can be tested against it. A new data category, affected group, model, recipient, country, purpose, scale, technology, retention period or failed TOM should raise a drift or review condition. The reviewer then determines whether the DPIA remains valid, requires an update or supports suspension.

7.4 From risk treatment to a statement of applicability

ISO/IEC 27701:2025 requires the organisation to determine controls necessary to implement privacy risk treatment, compare them with Annex A, and produce a statement of applicability that records controls, justification, implementation status and exclusions [6]. The framework generates this view from governed TOM and applicability decisions rather than maintaining an unrelated spreadsheet.

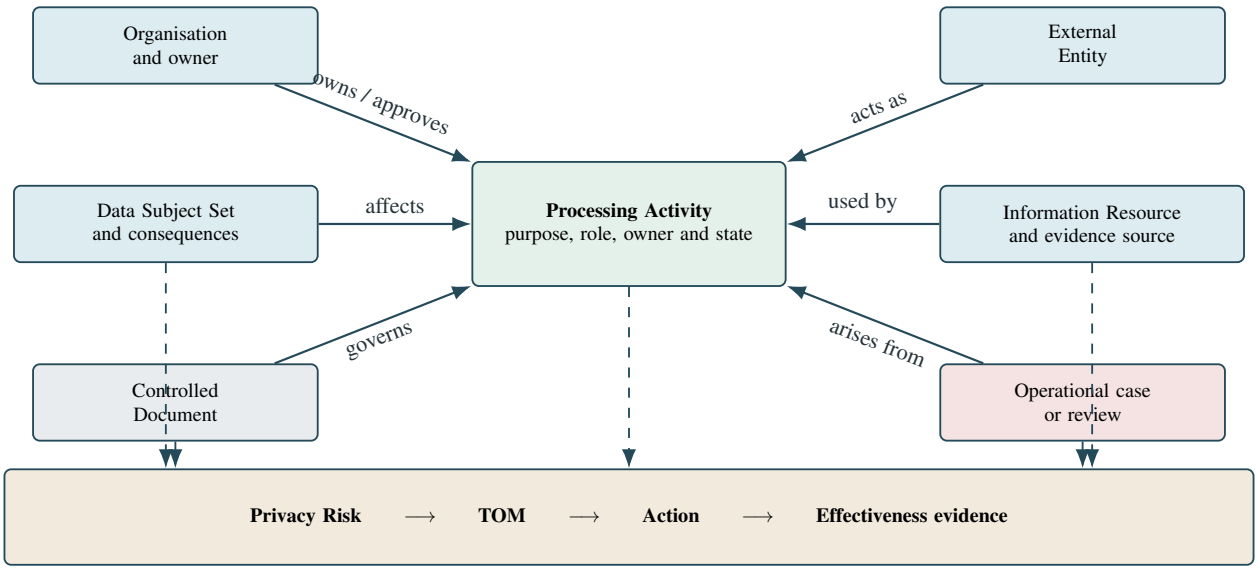

Figure 5: Processing Activity anchors a context graph without collapsing separately governed entities. Material links preserve role, scope, applicability and time.

The SoA record should identify the PIMS scope and version of the control set, applicability decision, controller or processor context, rationale, implementation state, linked TOMs, responsible owner, evidence, exceptions, residual Risk and approval. A control can be applicable even if implementation is incomplete. It can be not applicable only with a reason that remains valid for the stated scope. A change in role, processing or scope should trigger review of the relevant decision.

The SoA is an important claim boundary. Prudence can supply the structure, route decisions and generate a consistent view. The organisation must determine applicability, implement the measures and accept residual risk. A complete SoA generated from unsupported assertions is not evidence of an effective PIMS.

7.5 The complete risk-to-evidence chain

The intended chain is:

processing context → risk scenario → inherent analysis → treatment decision → TOM and Action → implementation evidence → effectiveness result → residual analysis → approval → monitoring and review.

Each transition has a named owner and date. Changes can enter at any point. New information may change the scenario or likelihood. A treatment action may be late. Evidence may show implementation failure. A control may work but reveal a different residual effect. An approval can expire or become conditional. Monitoring can reopen the assessment.

VIII. OPERATIONAL RIGHTS, INCIDENTS, PROCESSORS AND TRANSFERS

8.1 Data-subject requests as governed cases

The rights in Articles 12 to 22 require a service operation. The framework uses a DSR record with identity, received date, right, channels, controller context, requester and representative status, identity-verification position, scope, linked Processing Activities, Resources, Entities and recipients, searches and actions, exceptions or restrictions, extension decision, response, evidence and closure. A statutory clock and escalation state are calculated from the relevant date and jurisdiction.

The workflow should distinguish receipt from validation, search from legal decision, and response preparation from approved completion. An access request may require data from processors; an erasure request may involve lawful retention; restriction may affect downstream use; rectification or erasure may require notification to recipients under Article 19. The system must therefore support linked Actions and recipient coordination rather than a single "complete" checkbox.

The platform can calculate deadlines, identify likely systems, assign work and preserve the response package. It cannot establish identity safely without appropriate organisational procedure, decide an exception without legal judgement, find data in a system that is not linked or integrated, or ensure staff carry out the response. Closure should require evidence appropriate to the selected right and decision.

8.2 Personal-data breaches and the 72-hour decision

A personal-data breach workflow begins with awareness, not with a polished incident report. The Breach record should preserve when and how the organisation became aware, what is known and uncertain, affected data, people, Processing Activities, Resources and Entities, containment, risk to rights and freedoms, notification decision, reasons, authority communication, data-subject communication, processor or customer coordination, evidence, actions and lessons.

Article 33 creates a 72-hour notification expectation for a controller unless the breach is unlikely to result in risk to rights and freedoms; processors notify controllers without undue delay. Article 34 uses a high-risk threshold for communication to affected people [1]. EDPB guidance provides operational examples and emphasises recognition, documentation and reasoned notification decisions [31]. The platform should therefore display the elapsed time and decision status, not merely a final notification deadline.

An incident-management or security platform may remain authoritative for forensic facts, containment and technical evidence. Prudence governs the privacy assessment, legal role, notification and affected-processing context. The systems should be linked rather than forcing the DPO to recreate an entire investigation.

8.3 Processor engagement as a lifecycle

Processor governance is often treated as a signed agreement. The framework treats it as a relationship lifecycle: need and role identification; due diligence; instruction and purpose; data and data-subject scope; security and confidentiality; subprocessor position; location and transfers; assistance with rights, breaches and DPIAs; deletion or return; audit rights; approval; operation; periodic review; change; and exit.

The Entity, Processing Activity, Resource, Document, Transfer, TOM, Risk and Action records collectively support this lifecycle. Contract templates can cover repeatable Article 28 terms, but they do not

Table 3: Principal controlled entities and their control purpose

Controlled entity	Principal facts and decisions	Key relationships	Primary demonstrability purpose
Organisation and role	Legal identity, establishments, PIMS scope, policy, DPO and governance roles	Business units, owners, authorities, controller/processor contexts	Shows who is accountable and what the programme covers
External Entity	Legal identity, service, privacy role, locations, due diligence, contract and subprocessors	Processing Activities, Transfers, Documents, Resources	Supports Articles 26 and 28, recipient governance and supply-chain review
Processing Activity	Purpose, role, owner, data, people, source, recipient, retention, lawful basis, state	All contextual, documentary, risk and operational records	Operational inventory and source for controller/processor RoPA
Data Subject Set	Affected people, scale, location, vulnerability, expectations and possible consequences	Processing Activities, Risks, DPIAs, Requests, Breaches	Preserves the individual perspective in design and risk decisions
Information Resource	System or store, provider, location, data context, owner, access, deletion and evidence references	Processing Activities, DSRs, Breaches, TOMs	Makes operational scope, search, retention and security evidence traceable
Document	Type, scope, version, status, owner, approval, effective and review dates	Processing, Entities, Risks, Controls, Audits	Controls policies, notices, contracts and assessments without detaching them from use
Privacy Risk	Source, affected context, likelihood, consequences, criteria, treatment and residual decision	Data subjects, Processing, DPIA, TOMs, Actions, Evidence	Connects impact on people and organisational consequences to treatment
TOM	Control objective, design, owner, implementation, applicability and testing	Risks, Processing, Resources, SoA, Evidence	Represents the technical or organisational measure and whether it works
Privacy Action	Required change, owner, deadline, status, evidence and verification	Gaps, Risks, Audits, Reviews, Breaches	Turns findings and decisions into controlled improvement work
DSR	Requester, identity, right, scope, dates, searches, decisions, response and evidence	Processing, Resources, Entities, Recipients	Demonstrates operational execution of data-subject rights
Personal-data breach	Awareness, facts, affected data and people, risk, notification decisions, actions and evidence	Processing, Resources, Entities, Risks, Authorities	Preserves recognition, assessment, 72-hour decision and communication history
Audit or Review	Scope, criteria, participants, evidence, findings, conclusions and actions	PIMS objectives, Records, Risks, Controls, SoA	Supports monitoring, internal audit, management review and improvement

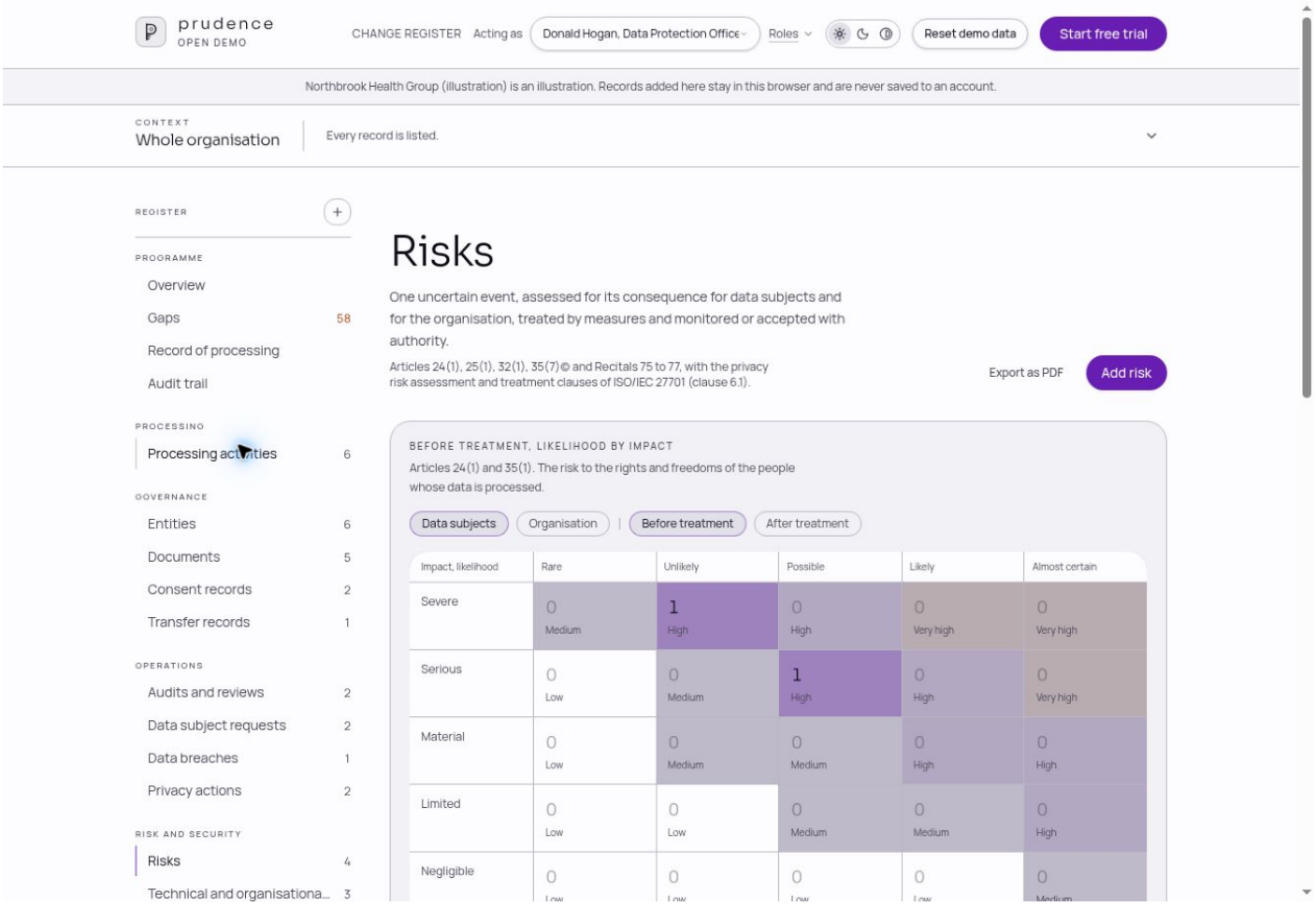

Figure 6: Illustrative risk register preserving consequences for data subjects and the organisation before and after treatment. The two perspectives remain visible rather than being averaged into a compliance score.

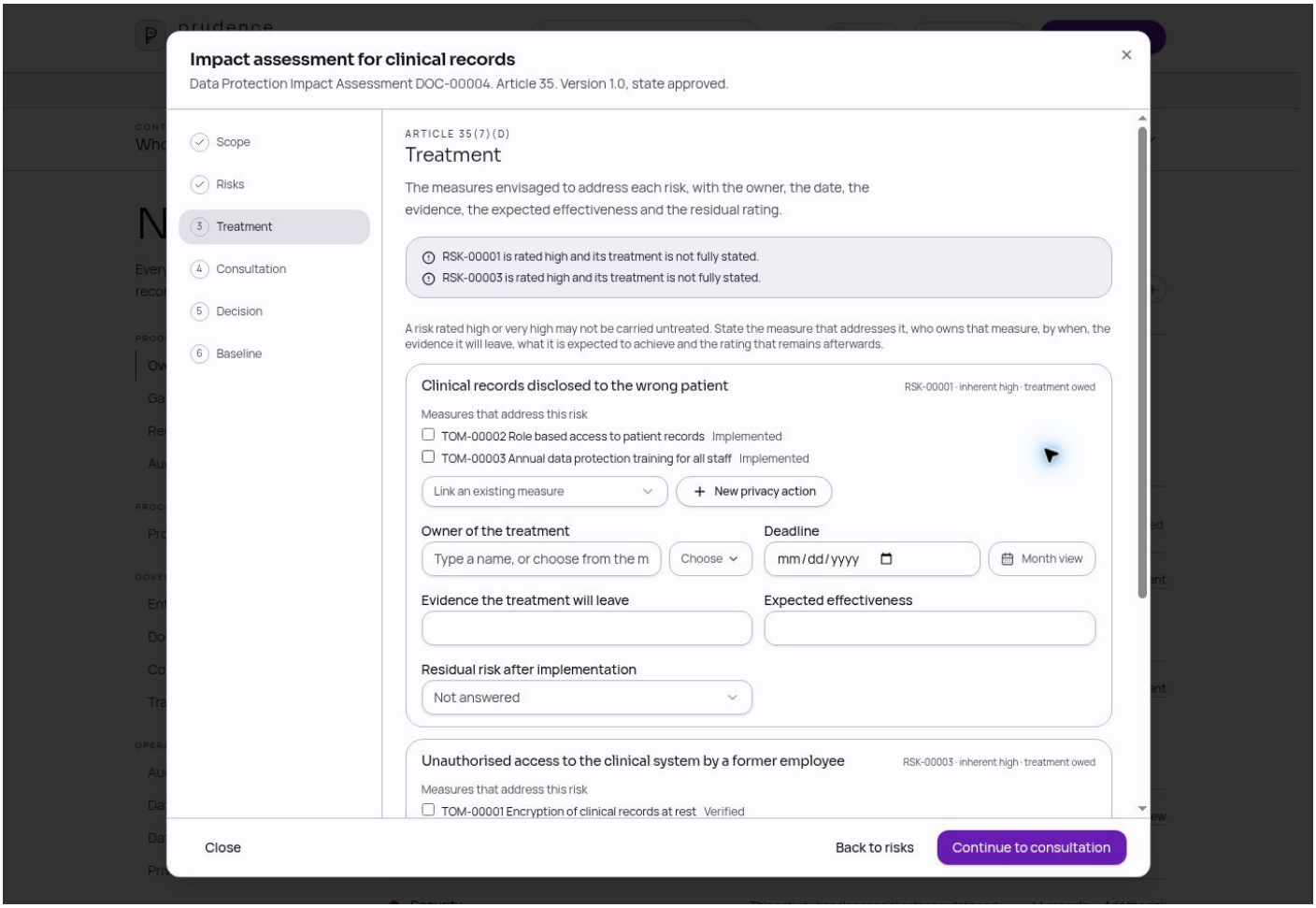

Figure 7: Illustrative DPIA treatment stage. Risks, TOMs, actions, owners, deadlines, evidence, effectiveness and residual conclusions are governed as connected records rather than flattened into assessment narrative.

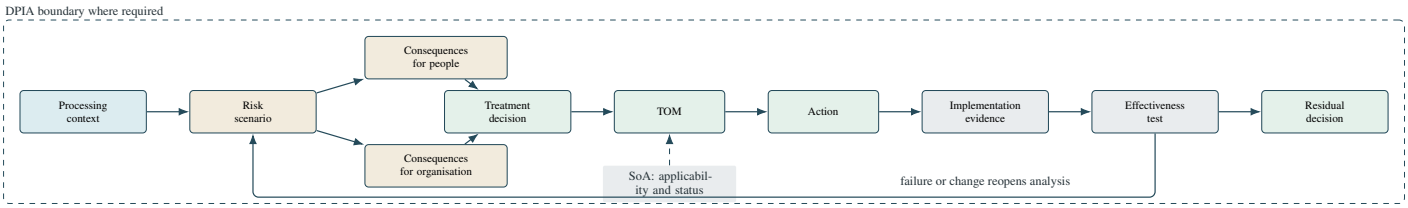

Figure 8: Privacy risk preserves consequences for people and the organisation, then connects treatment to implementation, effectiveness, residual decision, DPIA and statement of applicability.

establish that the chosen processor provides sufficient guarantees or follows the instructions. Due diligence evidence, unresolved exceptions, review dates and subprocessor changes should remain visible. EDPB Opinion 22/2024 further illustrates the controller's continuing accountability for processor and subprocessor arrangements [38].

8.4 Transfers and disclosures

A Transfer record should distinguish the factual movement or availability of personal data from the legal mechanism used to support it. It identifies exporter and importer roles, countries, Processing Activities, data and people, purpose, onward transfers, mechanism, supplementary measures, assessment, approval and review triggers. Different transfers involving the same supplier may have different purposes, roles or mechanisms.

The platform can control approved transfer documents, track assessment and expose a missing or stale mechanism. It cannot guarantee the law or practice of a third country, operate encryption or prevent unauthorised onward transfer. Those conclusions depend on legal analysis, supplier behaviour and technical controls, for which the Transfer and TOM records preserve the evidence path.

IX. ISO/IEC 27701 MANAGEMENT-SYSTEM INTEGRATION

9.1 Context, scope and interested parties

PIMS scope is a governance boundary, not a marketing description. It should identify organisational units, locations, products or services, controller and processor roles, categories of processing, interfaces with other management systems, exclusions and dependencies. The Organisation, business-unit, Entity, Processing Activity and Resource records provide the factual inventory from which the scope can be reasoned. Interested-party records and applicable-obligation references preserve customer, data-subject, authority, contractual and internal expectations.

The platform can generate a scope view and reveal processing outside it. Management must decide whether the scope is appropriate and must not use a narrow certificate boundary to imply broader organisational conformity. Changes to role, service, jurisdiction, acquisition or outsourcing should create a scope-review trigger.

9.2 Leadership, policy and assignment

Leadership is demonstrated through decisions and resources as well as a signed policy. Prudence can control the privacy policy, assign executive and operational roles, route approval, publish objectives and preserve management-review decisions. Mandatory owners across processing, Risk, TOM, Action, DSR, Breach and Document records show how the allocation works in practice.

The platform cannot create commitment, independence or resources. Senior management must set direction, resolve conflicts, support the DPO, accept appropriate residual risk and enforce completion. Evidence may include approved policy, meeting decisions, budget or staffing actions, objective status, escalations and closure of management actions.

9.3 Planning, risk and objectives

Clause 6 connects risks and opportunities, privacy risk assessment and treatment, the information-security programme, Annex A comparison, SoA, objectives and planned change [6]. The framework's Risk, TOM, Action, SoA and Objective records form the corresponding operational chain. Risk criteria, owners, approval authorities and review intervals should be controlled documented information. Objectives should state the intended result, indicator, baseline where relevant, target, owner, resources, due date and evaluation method.

Privacy objectives should not be limited to counts of documents. Useful examples include reducing overdue DSR actions, bringing high-risk processing under published DPIA baselines, obtaining current effectiveness evidence for critical TOMs, closing processor due-diligence exceptions, improving timeliness of processing-owner reviews or eliminating unapproved transfers. A target can create perverse incentives if interpreted mechanically. “Close all DSRs within one month” must not encourage premature closure or incomplete responses. Measures should be accompanied by quality and exception review.

9.4 Support: resources, competence, awareness, communication and documentation

Support controls are often template-capable but must show operation. A roles and responsibilities document, competence framework, awareness plan, communication procedure and documented-information procedure can be versioned, approved and reviewed in Prudence. People or role records, training evidence, assessment results, communication logs, publication history and overdue actions demonstrate implementation.

Competence is role-specific. A general annual privacy module may support awareness but does not establish that a DPO can advise on complex processing, that engineering staff can implement data minimisation, or that a DSR coordinator can apply exceptions. The organisation should define competence needed for material roles, evaluate current capability, plan development and record evidence. Where HR or learning systems are authoritative, Prudence should maintain the requirement, conclusion and evidence reference rather than duplicate personal files.

Documented information requires identity, review, approval, change control, availability, protection, retention and disposition. The Document record provides these controls for PIMS content. Records generated by workflows need their own immutable histories and retention rules. Export and backup are part of retrievability but do not replace access control, resilience or legal-hold implementation.

9.5 Operation

Operational planning and control is where the PIMS must become visible in daily work. Processing Activities establish the operating context; state transitions and conditional requirements provide gates; DSR and Breach records manage events; Entity and Transfer workflows govern external processing; DPIA, Risk, TOM and Action records govern risk treatment; and Documents preserve approved policy, notice, contract and assessment content.

The organisation should define which transitions require independence or approval, which gaps block progression, which conditions permit factual capture with escalation, and which changes trigger reassessment. Outsourced processes remain in scope where relevant. A processor relationship should therefore not disappear behind the existence of a supplier contract.

9.6 Performance evaluation and improvement

Monitoring should be derived from control objectives and material conditions. Candidate indicators include inventory review coverage, open high-risk gaps, DPIA baseline drift, overdue rights actions, breach-decision timeliness, processor exceptions, TOM evidence age, failed effectiveness tests, audit findings and corrective-action age. Each indicator should link to underlying records so management can distinguish trend from data-quality error.

An Audit or Review record should identify scope, criteria, independence, sample, evidence, findings and conclusion. Management review should address changes in context, interested-party expectations, privacy performance, objective progress, audit and incident results, resource adequacy, residual risk, opportunities and decisions. Findings should create Actions with root-cause analysis and effectiveness verification where appropriate. Continual improvement is evidenced by controlled changes and improved outcomes, not by a declaration that the system improves.

9.7 Templates as controlled implementation components

The question "Can this requirement be met with a template?" should be answered carefully. A policy, procedure, terms of reference, role description, agenda, contract clause or assessment form may be the correct artefact. It becomes credible when the template is adapted to scope, versioned, reviewed, approved, communicated, linked to affected records, used in the relevant workflow, supported by evidence and reviewed when its assumptions change.

Templates are therefore components of the control system, not substitutes for it. The framework distinguishes a template, an approved controlled document and an operational instance. A breach procedure is an approved document. A particular breach is an operational record. A DPIA template defines expected content. A published DPIA contains the analysis and decision for identified processing. A processor agreement template supports consistent terms. The executed agreement and due-diligence record govern the actual supplier.

X. DEMONSTRABILITY, ASSURANCE AND CHANGE

10.1 Immutable history and decision baselines

A current record is not sufficient for accountability where the organisation must explain earlier conduct. Governed changes should preserve actor, time, previous and new value, state transition and reason. Approved decisions should identify the exact baseline to which they apply. Supersession should not delete the earlier record.

The required depth follows materiality. Correcting a typographical error need not trigger a full privacy review. Changing purpose, lawful basis, data category, affected group, processor role, country, retention, technology, control or risk conclusion may. The system should classify or allow the reviewer to classify change significance and route affected records accordingly.

10.2 Review triggers and transitive impact

Periodic review is necessary but insufficient. The framework combines scheduled review with event-driven triggers. Relevant events include:

- new or changed purpose, product function, business process or legal basis;
- new data or data-subject category, especially sensitive or vulnerable contexts;
- change of processor, subprocessor, recipient, country or transfer mechanism;
- material change in system, model, interface, data source, access or retention;
- complaint, objection, request pattern, incident or breach;
- failed TOM, adverse audit finding or overdue treatment;
- change in law, guidance, contract or interested-party expectation;
- change in scale, likelihood, consequence or residual-risk acceptability; and
- PIMS scope, organisational or ownership change.

Trigger propagation should be transitive but reviewable. A Resource location change identifies linked Processing Activities. Those identify Transfers, Documents, Risks, DPIAs, Entities and TOMs that may be affected. The platform opens or proposes review conditions. A qualified owner decides materiality and records the outcome. This avoids both silent drift and indiscriminate invalidation.

10.3 Evidence without duplication

Prudence should be the authoritative system for privacy-governance context and decisions where designed to be so. It should not become a copy of every source system. Security configuration belongs in security and infrastructure tools. Executed contracts may belong in contract management. Workforce training details may belong in HR or learning systems. Product requirements and test results may belong in development or quality systems.

The framework uses controlled references and evidence conclusions. The TOM records what outcome is required, where it applies, which system holds objective evidence, when evidence was evaluated, by whom and with what conclusion. Critical evidence may also be attached or preserved where retention and accessibility justify it. The allocation should be documented so an auditor can navigate without accepting a broken hyperlink as evidence.

10.4 Exports and external assurance

Exports should be reproducible projections of governed records. Useful outputs include controller and processor RoPAs, processing details, risk and TOM registers, DPIA reports, DSR and Breach case files, Entity and Transfer registers, SoA, audit and management-review packs, open-gap reports and CSV backup. Each should identify scope and generation date.

An export is not stronger than its source. Therefore, review should begin by drilling from summary to record, then to decision and evidence. A polished PDF with unresolved gaps should not obscure them. Where the organisation chooses to share only part of a record for confidentiality or data minimisation, the system should preserve the complete internal baseline and record the redaction or projection.

10.5 Claim architecture

Three claims should be kept separate.

1. **Platform-capability claim:** Prudence provides structured records, relationships, workflows, controlled documents, risk and control management, evidence and outputs that support implementation and demonstration of GDPR and ISO/IEC 27701 requirements.
2. **Organisational compliance claim:** the customer concludes that its identified processing and practices comply with applicable GDPR duties, supported by current facts, decisions, controls and evidence.
3. **Certification claim:** an accredited certification body determines that the organisation's scoped PIMS conforms to ISO/IEC 27701 under the applicable certification arrangement.

The first can be demonstrated through product specification and testing. The second belongs to the controller or processor and remains subject to authority and court scrutiny. The third belongs to certification. Marketing language should not collapse them.

XI. ADOPTION PATTERNS

11.1 A proportionate sequence

The framework should be implemented in an order that reduces real risk and creates useful evidence early. The first objective is not to populate every field. It is to establish a truthful context and gain control of urgent obligations.

Stage 1: establish accountability. Define organisation and PIMS scope, assign executive and privacy roles, record controller/processor

Table 4: GDPR requirement families, framework mechanisms and retained human authority

GDPR requirement family	Principal framework mechanisms	What the structure can demonstrate	Decision or action that remains organisational
Principles, lawfulness and accountability, Arts. 5, 6, 9, 24	Processing Activity, lawful-basis fields, controlled assessments, owners, approvals, Risks, TOMs, reviews and history	Which purposes, legal bases, conditions, safeguards, owners and reviews support each activity	Whether the purpose and basis are valid, processing is fair and measures operate in reality
Transparency, Arts. 12-14	Document, Data Subject Set, Processing Activity, channel, version, publication evidence and review trigger	Which notice applies to which people and processing, when approved and how made available	Whether information is intelligible, accessible, complete and delivered at the right time
Rights, Arts. 15-22	DSR case, identity and scope, statutory clock, Resources, Entities, Actions, decisions, response and evidence	Receipt-to-response history and evidence for each request	Identity judgement, exception, substantive response and execution in source systems
Controller/processor allocation, Arts. 24, 26, 28, 29	Organisation, Entity, Processing relationship, due diligence, agreement, instructions, sub-processors and review	Factual role decision, approved terms, linked activities and unresolved exceptions	Correct role determination, sufficient guarantees and performance of contract/control obligations
Records of processing, Art. 30	Processing Activities and related Entities, data, people, recipients, transfers, retention and TOMs; controller/processor export	Current governed source and formal RoPA projection with ownership and history	Completeness and accuracy of inventory and any applicable exemption judgement
Security, Art. 32	Risks, TOMs, Resources, implementation/effectiveness evidence, failures and Actions	Applicability, design, ownership, evidence reference, latest test and residual position	Implementation and operation of security controls in technical and organisational environments
Breach, Arts. 33-34	Breach case, awareness time, risk decision, 72-hour clock, authority/person communication and evidence	Reasoned, timed privacy decision and complete case history	Detection, containment, forensic facts, notification judgement and actual communication
DPIA and prior consultation, Arts. 35-36	Screening, DPIA stages, inherited processing scope, Risk/TOM/Action, consultation, decision, baseline and drift	Why assessment was required, assessed context, treatment, advice, residual decision and review	Quality of analysis, acceptance authority, restriction of processing and consultation with authority
Data protection by design/default, Art. 25	Processing lifecycle gates, Data Subject Sets, Risks, TOMs, design evidence, effectiveness and change triggers	When privacy requirements and measures were considered, approved and tested	Product and process design, default configuration and real-world effectiveness
Transfers, Chapter V	Transfer, Entities, roles, mechanism, assessment, supplementary TOMs, approval and review	Which transfers exist, their mechanism, evidence, conditions and changes	Legal assessment of mechanism, third-country conditions and operation of supplementary measures
DPO, records and cooperation, Arts. 30, 37-39, 58	Governance document, role allocation, consultation, independent advice, review, reporting and export	DPO involvement, advice, response, reporting and access to current records	Independence, adequate resources, expert judgement and organisational cooperation

Table 5: ISO/IEC 27701:2025 management-system clauses 4 to 8 in the framework

Clause or control family	Requirement summary	Template-supported elements	Native or linked platform mechanisms	Residual organisational responsibility
4 Context of the organisation	Determine context, interested parties, PIMS scope and processes	Context methodology, scope statement, interested-party procedure	Organisation, business units, roles, Entities, Processing Activities, Resources, obligations and scope-review triggers	Select a credible scope, understand external/internal issues and operate required processes
5 Leadership	Demonstrate commitment, establish policy, roles, responsibility and authority	Privacy policy, governance charter, role descriptions	Controlled approval, owners on all material records, escalation, decision and management history	Provide authority, independence, resources and actual leadership behaviour
6.1 Risks and opportunities	Determine and address PIMS risks/opportunities; assess privacy risk; plan treatment and information security	Risk method, criteria, acceptance and treatment procedure	Risk register, dual consequences, TOMs, Actions, approval, evidence and review	Identify realistic scenarios, apply criteria, implement treatment and accept residual risk
6.1.3 SoA and treatment plan	Compare necessary controls with Annex A; justify inclusion/exclusion and implementation status	SoA methodology and standard control narratives	Applicability decision, TOM mapping, justification, status, evidence, exceptions and approval	Correctly determine necessary controls and ensure their effective implementation
6.2 Objectives	Establish measurable privacy objectives and plans	Objective policy and reporting template	Objectives, indicators, owners, due dates, resources, results and management review	Choose meaningful objectives, resource them and prevent metric gaming
6.3 Planning changes	Carry out PIMS changes in a planned manner	Change procedure	Change record, affected relationships, assessment, approval, conditions and post-change review	Decide change scope, implement safely and evaluate unintended effects
7 Support	Provide resources, competence, awareness, communication and controlled documented information	Competence matrix, awareness plan, communication and document-control procedures	Role requirements, training/evidence references, controlled Documents, publication and review	Supply people and budget, create competence, communicate and protect information
8 Operation	Plan, implement and control PIMS processes; perform risk assessment and treatment	Operating procedures and work instructions	Lifecycle gates, conditional requiredness, Risks, TOMs, Actions, DPIA, DSR, Breach, processor and Transfer workflows	Perform substantive work, make valid decisions and ensure controls operate outside the platform

Table 6: ISO/IEC 27701:2025 evaluation, improvement and Annex A controls in the framework

Clause or control family	Requirement summary	Template-supported elements	Native or linked platform mechanisms	Residual organisational responsibility
9.1 Monitoring and evaluation	Decide what to monitor and evaluate methods, timing and results	Metrics catalogue and reporting method	Record-derived indicators, evidence age, failed controls, statutory clocks, gap and objective trends	Interpret results, validate data quality and act on adverse findings
9.2 Internal audit	Conduct planned, objective audits and preserve results	Audit programme, procedure and checklist	Audit records, criteria, sample, evidence, findings, Actions and follow-up	Ensure auditor competence/independence and perform adequate testing
9.3 Management review	Review PIMS suitability, adequacy and effectiveness; decide changes and resources	Agenda and minutes template	Review inputs, linked indicators/findings/risks, decisions, owners and due dates	Conduct genuine review, challenge evidence and provide decisions/resources
10 Improvement	Address nonconformity, corrective action and continual improvement	Nonconformity and corrective-action procedure	Finding or gap, containment, cause, Action, effectiveness, closure and trend	Identify root causes, implement effective correction and sustain improvement
Annex A.1 PII controller controls	Govern purposes, lawfulness, consent, records, rights, design/default, sharing, transfer and disclosure	Notices, consent text, LIA, agreements, transfer/DPIA templates	Processing, Data Subject Set, Documents, Consent, DSR, Transfer, Risk/TOM and evidence	Establish lawful/fair processing and perform controller duties in practice
Annex A.2 PII processor controls	Govern customer instructions, terms, assistance, records, transfer/disclosure and return/disposal	Processing terms, assistance, deletion and customer-communication procedures	Entity/customer relationship, processor RoPA, instruction, DSR/Breach assistance, Transfer and exit Actions	Act only on lawful instructions, provide assistance and execute return/deletion
Annex A.3 security considerations	Maintain adequate information-security controls supporting privacy	Information-security policy set and control descriptions	TOMs, Resource links, risk mapping, external evidence, effectiveness and failures	Operate the ISMS/security programme and provide reliable technical evidence

Table 7: Allocation of authority among the organisation, Prudence and connected systems

Subject	Prudence authority	Connected-system authority	Human or governance authority
Privacy context and role	Organisation, Processing Activity, Entity relationship and documented decision	Corporate, product or contract data where authoritative	Controller/processor, purpose and scope determination
Lawful basis and transparency	Applicable fields, assessment/document link, approval, publication evidence and review	Website/content platform may prove delivery; consent service may prove event	Legal conclusion, fairness, clarity and choice design
Privacy risk and DPIA	Risk scenario, dual impact, treatment, decision, baseline and review	Product/security/quality evidence may substantiate facts and measures	Risk criteria, judgement, consultation and residual acceptance
Technical and organisational measures	Applicability, objective, owner, implementation/effectiveness conclusion and evidence reference	Identity, cloud, security, HR, quality or operations systems hold implementation evidence	Control design, operation, testing and remediation
Rights and breach privacy workflow	Case, statutory clock, scope, decision, communication and evidence	Service desk, data systems and security incident platform may execute searches or response	Identity, exceptions, risk, notification and substantive response decisions
Processor and transfer governance	Role, due diligence status, linked processing, agreement/assessment control and changes	Contract repository, vendor-management and security tools may hold primary evidence	Selection, negotiation, legal assessment, instruction and ongoing oversight
PIMS assurance	Objectives, indicators, audits, reviews, findings, SoA, actions and history	Finance, HR, ISMS and other systems supply selected evidence	Audit independence, management challenge, resources, corrective action and certification scope

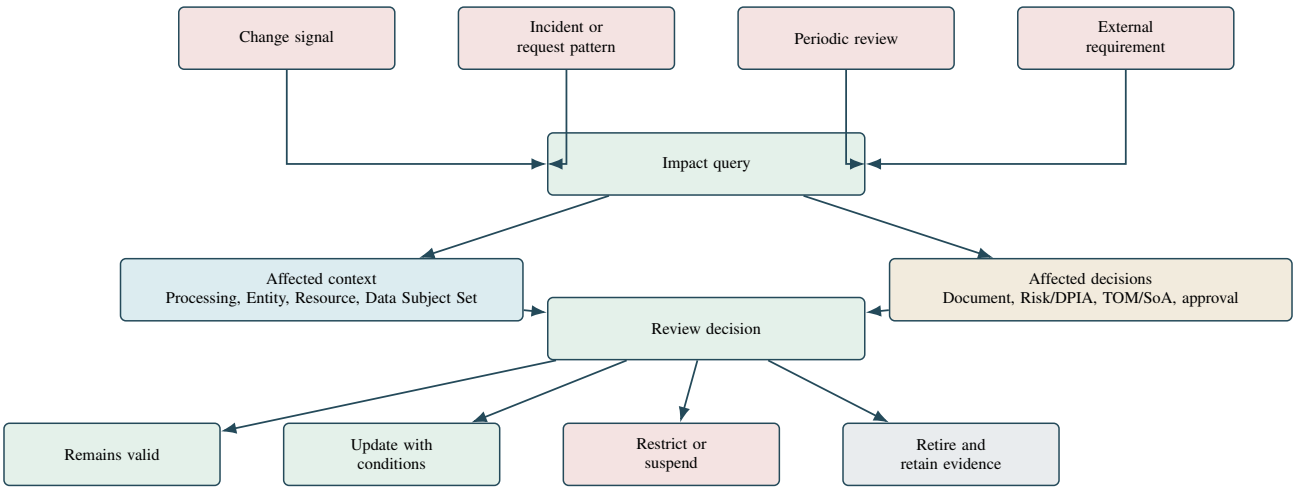

Figure 9: Scheduled and event-driven signals identify affected context and decisions. Review records whether the baseline remains valid, needs conditions, must be restricted or should be retired.

contexts, approve a concise policy, set risk criteria and establish breach and DSR routes.

Stage 2: map material processing. Capture operational Processing Activities, Data Subject Sets, Entities and Resources. Generate the first RoPA and expose missing owners, bases, retention, processor terms, transfers and high-risk screening.

Stage 3: control the highest risks. Complete or update DPIAs, transfer assessments and processor due diligence. Create Risks, TOMs and Actions with implementation and effectiveness evidence. Decide whether processing must be restricted while gaps are addressed.

Stage 4: operate and integrate. Use DSR, Breach, consent, Transfer, Audit and Review workflows. Connect authoritative evidence systems. Introduce event-driven review and owner attestations.

Stage 5: assure and improve. Complete SoA, internal audit, management review, objective evaluation, nonconformity and corrective-action cycles. Prepare a certification or external-assurance pack if this supports organisational objectives.

11.2 Worked pattern: small contract research organisation

A small CRO may process investigator contacts, candidate or employee information, sponsor data, trial-participant coded data and operational system logs. It may act as controller for employment and business operations, processor for sponsor-directed trial services, and controller or joint controller in selected contexts. The central governance risk is role and scope ambiguity combined with high sensitivity and multiple systems or subcontractors.

The initial Prudence implementation should establish separate Processing Activities for material purposes rather than one activity called "clinical research". Trial-specific or service-family records can share controlled templates and Entities while preserving sponsor instructions, data categories, countries, retention and security context. Participant groups should be represented as Data Subject Sets with vulnerability and consequence considerations. Each study or platform Resource should identify location and access context. Processor agreements, subprocessor approval and transfer positions should be linked to the affected activity.

Likely high-risk activities should be screened early. A DPIA can be derived from the Processing Activity, allowing the factual operating baseline to populate scope. Risks should consider re-identification, unauthorised disclosure, protocol or purpose deviation, excessive access, data-quality consequences, retention, participant expectations and cross-border availability. TOMs may reference the quality and information-security systems for access, coding, validation, backup, incident response and supplier control. The DPO and, where applicable, sponsor responsibilities should be explicit.

This sequence gives the founder a defensible management view: which studies or services are in scope, where critical gaps exist, who owns them, whether required assessments and terms are approved, which measures lack evidence and which statutory cases are open. It does not require a large compliance department. It requires disciplined ownership of a finite set of material records.

11.3 Worked pattern: young fintech

A young fintech may collect identity, account, transaction, device, fraud, credit or behavioural information through its own interfaces and external providers. Purposes can evolve quickly as product teams test onboarding, personalisation, risk, support and analytics. The central governance risk is purpose and data expansion outpacing notice, legal basis, processor, transfer, retention and DPIA decisions.

Processing Activities should therefore be purpose-specific and linked to product Resources, data sources and recipients. Product-change review should ask whether a feature changes purpose, data, affected groups, automated decision consequences, source, recipient, retention or geography. Legitimate-interests assessments, consent decisions and notices should be controlled Documents linked to the relevant activity. High-risk or automated decision contexts should route DPIA and rights review.

The Risk model should preserve consequences for people, such as exclusion, incorrect adverse decisions, financial impact, manipulation, surveillance or inability to contest, separately from organisational regulatory and commercial consequences. TOMs may include data minimisation, segregation, explainability or contest routes, access, monitoring, testing, fraud safeguards and retention automation. Evidence remains in product, data and security systems but is reviewed through the privacy control record.

The resulting system allows the founder and DPO to discuss product changes using the same governed context. Privacy review is not a late legal ticket; it is a controlled impact decision connected to release and later signals.

11.4 Worked pattern: the experienced DPO

An experienced DPO often inherits an inventory, policies, a vendor list, open requests, historic DPIAs and audit actions maintained in different formats. The first value of the framework is not teaching the law. It is giving the DPO a reliable map of accountable owners and decision state.

Migration should preserve authoritative artefacts while normalising their control metadata. Processing Activities receive owners and review states. Existing DPIAs and LIAs become controlled Documents linked to the processing they assess. Open requests and breaches become cases with dates, decisions and evidence. Risks and controls are

de-duplicated carefully so that one TOM can apply to multiple activities without losing local exceptions. Stale, contradictory or unsupported conclusions become gaps rather than being silently "cleaned".

The DPO can then use dashboards for prioritisation, not as a substitute for judgement; route consultations and record advice; monitor overdue owner work; select samples for internal review; prepare management reporting from live records; and produce targeted evidence for customers, authorities or auditors. The platform supports independence by making advice, management response and unresolved conditions visible. Organisational position and resources still determine whether that independence is effective.

XII. DISCUSSION

The Prudence Framework is deliberately more structured than a document repository and less presumptuous than an automated legal decision-maker. Its value lies in converting obligations into an inspectable operating model while keeping substantive authority where it belongs.

The concept of accountability continuity extends familiar traceability ideas. Privacy compliance requires more than mapping a clause to a policy. The material chain connects processing facts to a legal and governance decision, then to risk, control, evidence, approval, operation and change. This is why the same data model can serve both GDPR accountability and ISO/IEC 27701 management-system operation. The Regulation determines legal duties; the standard supplies organisational discipline; the framework connects both to daily work.

The Processing Activity is a strong anchor because it concentrates the regulated context. It should not become a monolithic form. Related entities remain separately governed so they can be reused, reviewed and changed without duplication. A processor can serve many activities. A Resource can hold data for many purposes. A Data Subject Set can be affected by several activities. A TOM can treat several Risks. Controlled relationships preserve these cardinalities and make impact analysis possible.

The risk design addresses a frequent defensibility weakness. Many compliance programmes rate risks through the organisation's exposure and use the result as a proxy for harm to people. Keeping both consequence views visible improves management discussion and aligns more closely with GDPR and current ISO privacy-risk thinking. Connecting treatment to objective effectiveness evidence further reduces the gap between a stated safeguard and an operating control.

The DPIA pattern is equally important. Organisations need to inventory what actually happens, including non-compliant or incompletely assessed processing. A platform that permits only approved processing to be recorded as operational will produce a false inventory. A platform that permits operation without surfacing the missing assessment is weak. The framework's distinction between factual state and governance authorisation enables pragmatic remediation while keeping the compliance concern explicit. This is an example of usability strengthening, rather than diluting, accountability.

The framework also clarifies the role of templates. Privacy governance contains repeatable artefacts, and forcing every organisation to draft from a blank page would be wasteful. Templates are defensible where they are controlled, contextualised and used. They are weak where the existence of a file is treated as proof that a process operates. The platform should therefore combine a library with application, review and evidence.

For commercial use, the strongest claim is not that Prudence "does GDPR" or is itself "ISO/IEC 27701 compliant". The stronger and more credible claim is that it provides a purpose-built structure through which an organisation can establish, operate and demonstrate a privacy programme: governed processing context; linked legal and risk decisions; controlled workflows; assigned action; evidence and effectiveness; management-system review; and exportable assurance. That claim can be inspected feature by feature.

The approach is likely to be most valuable where processing is material but privacy resources are constrained, or where an experienced DPO must coordinate many owners. A small CRO or fintech gains proportional discipline and visibility. A DPO gains reliable operational context, escalation and reporting. Larger organisations may use the same model as a privacy control plane that references authoritative enterprise systems rather than replacing them.

Several implementation choices require care. Requiredness should be conditional and state-based, not indiscriminate. Dashboards should link to records rather than advertise unsupported scores. Notifications should prioritise statutory and risk-critical conditions. Permissions should protect confidential assessments without isolating the DPO. Integrations should preserve evidence identity and freshness. Terminology should distinguish current fact, approval and legal conclusion.

XIII. LIMITATIONS AND FUTURE WORK

The framework does not validate the truth or completeness of customer information. Required fields can improve consistency, but users can still make incorrect role, lawful-basis, transfer, risk or applicability decisions. Workflow completion does not prove fair processing, effective security or respect for rights. Assurance requires sampling and testing beyond the platform.

The legal analysis is centred on the EU GDPR and current ISO/IEC 27701. National law, sector rules, employment law, clinical-research requirements, financial regulation, ePrivacy rules and other jurisdictions may add or alter duties. The data model is designed to carry applicable obligations and context, but those overlays require competent interpretation.

ISO/IEC 27701:2025 is recent. Certification practice, sector interpretation and integration patterns will continue to mature. The mapping in this paper should therefore be tested with organisations, DPOs, auditors and certification professionals across controller and processor scopes. Particular research questions include whether the framework reduces time spent reconstructing evidence; improves completeness and timeliness of review; increases detection of change impact; and supports better-quality risk and DPIA decisions.

Future platform work can deepen evidence integration without turning Prudence into a copy of source systems. Useful directions include signed or API-verifiable evidence references, configurable freshness rules, processor and subprocessor change feeds, product-release privacy gates, data-catalogue integration, jurisdictional overlays, sampled control testing and management-review analytics. Any automated recommendation should show its rule and source, preserve human decision authority and avoid representing legal judgement as deterministic.

The framework would also benefit from controlled vocabularies for consequence domains, rights search scopes, TOM outcomes and review triggers, provided they remain adaptable. Excessive standardisation can suppress context. The objective is comparable reasoning, not identical answers.

XIV. CONCLUSIONS

Data protection becomes demonstrable when an organisation can connect what it does with personal data to why it does it, who is responsible, which people are affected, which decisions and risks apply, what controls have been implemented, whether those controls work and which change requires reconsideration. GDPR accountability and ISO/IEC 27701 management-system conformity both depend on that continuity.

The Prudence Framework provides a systematic architecture for maintaining it. Context establishes applicability. Governed records preserve facts and decisions. Operational workflows execute rights, incidents, processors, transfers and reviews. Privacy Risks remain connected to consequences for people and the organisation. TOMs and Actions connect treatment to implementation and effectiveness. Histo-

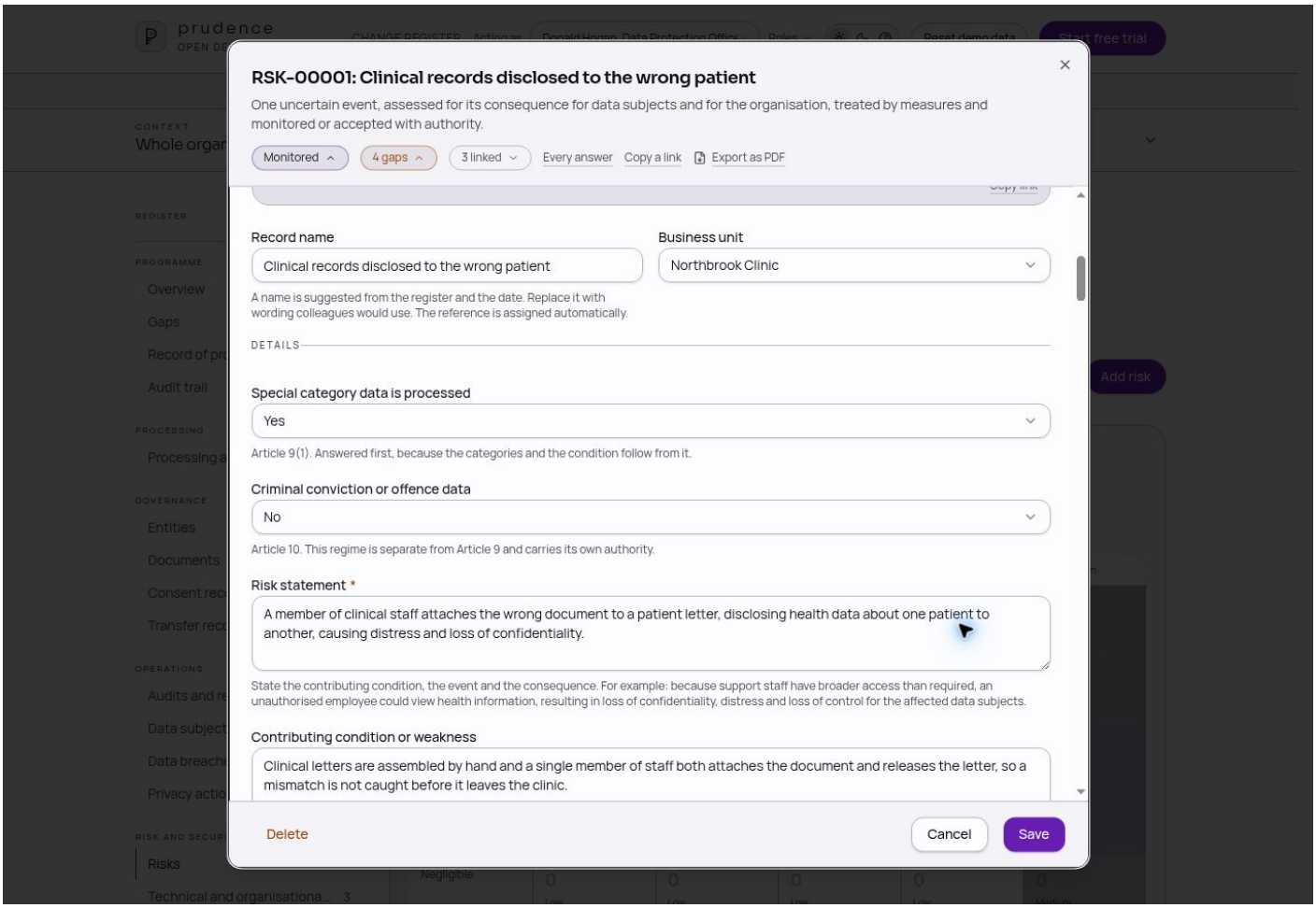

Figure 10: Illustrative route to a governed risk decision. Missing DPIA, DPO consultation, treatment effectiveness and approval are exposed as explicit conditions rather than left in narrative notes.

Table 8: Progressive adoption by organisational need

Stage	Small data-intensive company	Experienced DPO or established programme	Minimum evidence of completion
1 Accountability	Define scope, founder/executive accountability, DPO arrangement and urgent case routes	Confirm mandate, independence, governance forums, reporting and escalation	Approved scope/policy, assigned roles, DSR and breach route tested
2 Processing context	Capture few material purposes, systems, people, suppliers and countries	Consolidate inventories, resolve duplicates and assign record owners	Current RoPA projection, coverage review and named gaps
3 Risk and decisions	Prioritise sensitive/high-risk processing, key processors/transfers and critical TOMs	Normalise DPIA, LIA, transfer, Risk and TOM decisions; preserve exceptions	Published baselines, approved treatment, evidence for critical controls
4 Operation	Use cases and clocks; connect product/security evidence	Integrate service, security, vendor, HR and quality evidence and change routes	Sampled DSR/Breach cases, effective links and event-triggered reviews
5 Assurance	Management review, focused internal audit and improvement plan	SoA, audit programme, objectives, trends, corrective actions and certification readiness	Review decisions, closed actions with effectiveness and current assurance pack

ries, triggers and exports preserve accountability over time. The PIMS layer supplies leadership, objectives, assurance and improvement.

Prudence is the reference implementation of this architecture. Its appropriate claim is enabling rather than absolute: it gives controllers and processors a controlled structure through which to implement, operate and demonstrate their privacy programme. Compliance remains the result of accurate facts, sound judgement, effective measures and responsible organisational behaviour. Certification remains a conclusion about a scoped PIMS. By making those responsibilities visible and evidence-bearing, the framework offers a practical route between generic guidance and daily privacy work.

REFERENCES

[1] European Parliament and Council, "Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data," *Official Journal of the European Union*, L 119, 4 May 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[2] Article 29 Data Protection Working Party, "Opinion 3/2010 on the principle of accountability," WP 173, 13 July 2010. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf

[3] European Data Protection Board, "Guidelines 4/2019 on Article 25: Data Protection by Design and by Default," version 2.0, 20 October 2020. https://www.edpb.europa.eu/system/files/documents/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

[4] European Commission, "Second Report on the application of the General Data Protection Regulation," COM(2024) 357 final, 25 July 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0357

[5] European Data Protection Board, "2023 Coordinated Enforcement Action: Designation and Position of Data Protection Officers," adopted 16 January 2024. https://www.edpb.europa.eu/system/files/documents/2024-01/edpb_report_20240116_cef_dpo_en.pdf

[6] ISO/IEC 27701:2025, *Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance*. Geneva: International Organization for Standardization, 2025. https://www.iso.org/standard/27701

[7] ISO/IEC 29100:2024, *Information technology — Security techniques — Privacy framework*. Geneva: International Organization for Standardization, 2024. https://www.iso.org/standard/85938.html

[8] ISO/IEC 27557:2022, *Information security, cybersecurity and privacy protection — Application of ISO 31000:2018 for organizational privacy risk management*. Geneva: International Organization for Standardization, 2022. https://www.iso.org/standard/71675.html

[9] ISO/IEC 29134:2023, *Information technology — Security techniques — Guidelines for privacy impact assessment*. Geneva: International Organization for Standardization, 2023. https://www.iso.org/standard/86012.html

[10] National Institute of Standards and Technology, *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0*, NIST CSWP 10, 16 January 2020. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

[11] European Union Agency for Network and Information Security, *Privacy and Data Protection by Design — from policy to engineering*, December 2014. https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

[12] European Union Agency for Cybersecurity, *Data Protection Engineering: From Theory to Practice*, January 2022. https://www.enisa.europa.eu/publications/data-protection-engineering

[13] S. Spiekermann and L. F. Cranor, "Engineering privacy," *IEEE Transactions on Software Engineering*, vol. 35, no. 1, pp. 67–82, 2009. doi:10.1109/TSE.2008.88.

[14] J.-H. Hoepman, "Privacy design strategies," in *ICT Systems Security and Privacy Protection*, IFIP AICT 428, pp. 446–459, 2014. doi:10.1007/978-3-642-55415-5_38.

[15] S. Gürses and J. M. del Álamo, "Privacy engineering: Shaping an emerging field of research and practice," *IEEE Security & Privacy*, vol. 14, no. 2, pp. 40–46, 2016. doi:10.1109/MSP.2016.37.

[16] N. Notario et al., "PRIPARE: Integrating privacy best practices into a privacy engineering methodology," in *2015 IEEE Security and Privacy Workshops*, pp. 151–158, 2015. doi:10.1109/SPW.2015.22.

[17] K. Bednar, S. Spiekermann and M. Langheinrich, "Engineering privacy by design: Are engineers ready to live up to the challenge?" *The Information Society*, vol. 35, no. 3, pp. 122–142, 2019. doi:10.1080/01972243.2019.1583296.

[18] L. H. Iwaya, M. A. Babar and A. Rashid, "Privacy engineering in the wild: Understanding the practitioners' mindset, organisational aspects, and current practices," *IEEE Transactions on Software Engineering*, vol. 49, no. 9, pp. 4324–4348, 2023. doi:10.1109/TSE.2023.3290237.

[19] Y.-S. Martin and A. Kung, "Methods and tools for GDPR compliance through privacy and data protection engineering," in *2018 IEEE European Symposium on Security and Privacy Workshops*, pp. 108–111, 2018. doi:10.1109/EuroSPW.2018.00021.

[20] V. Ayala-Rivera and L. Pasquale, "The grace period has ended: An approach to operationalize GDPR requirements," in *2018 IEEE 26th International Requirements Engineering Conference*, pp. 136–146, 2018. doi:10.1109/RE.2018.00023.

[21] S. Sirur, J. R. C. Nurse and H. Webb, "Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation," in *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*, pp. 88–95, 2018. doi:10.1145/3267357.3267368.

[22] D. Torre et al., "Using models to enable compliance checking against the GDPR: An experience report," in *2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems*, pp. 1–11, 2019. doi:10.1109/MODELS.2019.00-20.

[23] H. Li, J. Werner, N. A. Ernst and D. Damian, "Towards privacy compliance: A design science study in a small organisation," *Information and Software Technology*, vol. 146, 106868, 2022. doi:10.1016/j.infsof.2022.106868.

[24] N. A. Zaguir, S. T. de Magalhães and R. O. Spinola, "Challenges and enablers for GDPR compliance: Systematic literature review and future research directions," *IEEE Access*, vol. 12, pp. 81608–81630, 2024. doi:10.1109/ACCESS.2024.3406724.

[25] G. A. Teixeira, M. M. da Silva and R. Pereira, "The critical success factors of GDPR implementation: a systematic literature review," *Digital Policy, Regulation and Governance*, vol. 21, no. 4, pp. 402–418, 2019. doi:10.1108/DPRG-01-2019-0007.

[26] A. Negri-Ribalta, M.-O. Lombard-Platet and C. Salinesi, "Understanding the GDPR from a requirements engineering perspective: a systematic mapping study," *Requirements Engineering*, vol. 29, pp. 523–549, 2024. doi:10.1007/s00766-024-00423-4.

[27] M. Rhahla, F. Allegue and T. Abdellatif, "Guidelines for GDPR compliance in Big Data systems," *Journal of Information Security and Applications*, vol. 61, 102896, 2021. doi:10.1016/j.jisa.2021.102896.

[28] European Data Protection Board, "Guidelines 07/2020 on the concepts of controller and processor in the GDPR," version 2.1, 7 July 2021. https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf

[29] Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment and determining whether processing is likely to result in a high risk," WP 248 rev.01, 4 October 2017. https://ec.europa.eu/newsroom/article29/items/611236

[30] European Data Protection Board, "Guidelines 01/2022 on data subject rights — Right of access," version 2.1, adopted 28 March 2023. https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf

[31] European Data Protection Board, "Guidelines 9/2022 on personal data breach notification under GDPR," version 2.0, 4 April 2023. https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf

[32] Information Commissioner's Office, "Guide to accountability and governance." https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/

[33] European Data Protection Board, "Data protection guide for small business." https://www.edpb.europa.eu/sme-data-protection-guide/home_en

[34] Organisation for Economic Co-operation and Development, *The OECD Privacy Framework*, 2013. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[35] E. Saltarella, G. Desolda and R. Lanzilotti, "Privacy design strategies and the GDPR: A systematic literature review," in *Human-Computer Interaction — INTERACT 2021*, LNCS 12788, pp. 241–257, 2021. doi:10.1007/978-3-030-77392-2_16.

[36] Article 29 Data Protection Working Party, "Guidelines on transparency under Regulation 2016/679," WP260 rev.01, 11 April 2018. https://ec.europa.eu/newsroom/article29/items/622227

[37] Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers," WP243 rev.01, 5 April 2017. https://ec.europa.eu/newsroom/article29/items/612048

[38] European Data Protection Board, "Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s)," 7 October 2024. https://www.edpb.europa.eu/system/files/2024-10/edpb_opinion_202422_relianceonprocessors-sub-processors_en.pdf

[39] Runciter, "Prudence documentation: Overview," accessed 2 August 2026. https://runciter.tech/docs/overview

[40] Runciter, "Prudence documentation: Register reference," accessed 2 August 2026. https://runciter.tech/docs/reference/registers

[41] Runciter, "Prudence documentation: Compliance guide," accessed 2 August 2026. https://runciter.tech/docs/reference/compliance-guide