# DHF Impact and Actions Recommendation – ISO/IEC 29100:2024

**Gap Assessment:** ISO/IEC 29100:2020 versus ISO/IEC 29100:2024

**Document Type:** DHF / Privacy-by-Design Impact Analysis

**Standard Reference:** ISO/IEC 29100:2024 – Information technology – Security techniques – Privacy framework

**Date:** June 22, 2026

**Revision:** 01

## Executive summary

ISO/IEC 29100:2024 retains the core privacy framework and 11 privacy principles from the 2020 edition, while refining references, clarifying wording, and strengthening integration with ISO/IEC 27000-based ISMS practices. The attached comparison concludes that the 2024 revision introduces mostly incremental updates rather than new mandatory elements, but those updates still affect DHF documentation, privacy governance, risk linkage, and evidence of privacy-by-design implementation.

The main DHF impact areas are alignment with ISMS references, clearer controller and third-party accountability, stronger handling of unsolicited and sensitive PII, principle-based alignment for collection limitation and data minimization, and more explicit privacy policy, transparency, and enforcement documentation.

## Key changes and DHF impact

### 1. Framework overview and ISMS integration

The comparison notes that ISO/IEC 29100:2024 now aligns the privacy framework with ISO/IEC 27000 and the broader ISMS ecosystem, while the 2020 version relied more on WG 5 SD2 references. This means the DHF should no longer present privacy as a standalone layer; instead, privacy requirements, risks, and controls should be traceable to the same management system structure used for information security.

**DHF impact:**

- Update DHF planning and privacy framework documents to reference ISO/IEC 27000-aligned ISMS artifacts.
- Add traceability between privacy requirements, ISMS controls, and risk assessments.
- Revise design review criteria so privacy design decisions are assessed alongside security design decisions.

| Action | Timeline | Owner | Priority |
|---|---|---|---|
| Update DHF planning documentation to reference ISO/IEC 29100:2024 and ISO/IEC 27000-aligned ISMS documents | 2–4 weeks | Privacy/ISMS Lead | Critical |
| Create a privacy-to-ISMS traceability matrix | 4 weeks | Quality/Risk | High |
| Update design review checklists to include ISMS-linked privacy controls | 4–6 weeks | Quality/Engineering | High |

## 2. Roles and accountability

The attached comparison shows that the actor model remains stable across principals, controllers, processors, and third parties, but 2024 places stronger emphasis on controller accountability and proactive safeguards. It also reiterates that third parties receiving PII generally assume controller responsibilities rather than acting under the original controller's authority.

**DHF impact:**

- Refresh system context diagrams and data-flow documents to classify each actor as controller, processor, or third party.
- Update accountability sections in design inputs, risk files, and supplier controls to reflect controller-led safeguard responsibilities.
- Ensure contractual documents and supplier qualification records reflect role-specific privacy obligations.

| Action | Timeline | Owner | Priority |
|---|---|---|---|
| Update actor-role mapping across architecture and data-flow documents | 3 weeks | Privacy Architect | Critical |
| Review supplier and third-party records for controller/processor role alignment | 6 weeks | Legal/Procurement | High |

| | | | |
|---|---|---|---|
| Add role-accountability checkpoints to privacy design reviews | 4 weeks | Privacy Officer | High |

## 3. Recognizing PII, unsolicited PII, and sensitive PII

The comparison says that the core recognition of PII is substantively unchanged, but 2024 stresses ICT transparency and user control when determining identifiability. It also highlights privacy-by-design safeguards for unsolicited PII and maintains stronger protection expectations for sensitive and inferred PII categories.

**DHF impact:**

- Update design inputs so systems explicitly identify direct identifiers, indirect identifiers, linkable information, metadata, unsolicited PII, and sensitive/inferred PII categories.
- Expand risk analysis to cover free-text capture, metadata leakage, hidden PII, and sensitive inference risks.
- Add UI and system requirements for transparency, preference management, and user awareness about PII handling.

| Action | Timeline | Owner | Priority |
|---|---|---|---|
| Revise PII classification rules in requirements and architecture records | 4 weeks | Privacy Analyst | High |
| Update risk assessments for unsolicited and inferred sensitive PII scenarios | 4–6 weeks | Risk Manager | High |
| Add transparency and user-control requirements to product specs and UX criteria | 6 weeks | Product/UX | High |

## 4. Safeguarding factors and privacy-by-design controls

The 2024 edition keeps legal, contractual, business, and other safeguarding factors largely intact, but it updates wording to connect business-driven decisions more explicitly to collection limitation and data minimization principles. It also maintains that privacy safeguards should be identified before ICT systems are designed or changed and should be driven by risk management.

**DHF impact:**

- Show in the DHF that business needs such as analytics, personalization, or operational reporting are constrained by documented minimization rules.
- Link each major privacy safeguard to legal, contractual, business, and user-preference drivers in the risk file or design rationale.
- Confirm that privacy controls are defined during design input and design review stages, not added only during validation or audit preparation.

| Action | Timeline | Owner | Priority |
|---|---|---|---|
| Update design inputs to justify each data element against business purpose and minimization principles | 6 weeks | Product/Business Analysis | Critical |
| Expand risk-control rationale to show legal, contractual, and user-preference factors | 6 weeks | Risk/Privacy | High |
| Add privacy-by-design gate criteria to change control and design change procedures | 4 weeks | Quality Systems | High |

## 5. Privacy policies, transparency, and notices

The comparison states that 2024 continues to distinguish internal privacy policies from external privacy policies or notices, while emphasizing documented enforcement measures such as access controls, audits, and communication. The openness, transparency, and notice principle also remains substantively the same, although it is reformatted and clarified in 2024.

**DHF impact:**

- The DHF should identify which requirements are fulfilled through internal policy controls and which are fulfilled through user-facing notices and operational disclosures.
- Verification evidence should show that transparency content, notice logic, access rights, and communications are implemented and maintained.
- Governance records should demonstrate top-management approval and continual improvement linkage for privacy policies.

| Action | Timeline | Owner | Priority |
|---|---|---|---|
| Update internal and external privacy policy references in DHF and traceability records | 4 weeks | Privacy Officer | High |