Introduction to ISO/IEC 27560-1: The Digital Public Privacy Standard

by Mark Lizar, 0PN: Digital Transparency Lab

Tagline: "It's not fair or trustworthy, if it's not Transparent First."

What Digital Public Privacy Means

ISO/IEC 27560-1 establishes **digital public privacy infrastructure**—treating transparency as public infrastructure rather than private property. Like traffic signs or food safety labels, controller accountability information becomes standardized, independently verifiable, and universally accessible.

Public Infrastructure Characteristics:

- **Standard location**: /.well-known/transparency/notice.txt (like safety data sheets)
- **Machine-readable format**: JSON structure enabling automated verification

- **Anonymous accessibility**: No authentication required to verify controller accountability
- **Universal baseline**: Convention 108+ treaty as common standard across jurisdictions
- **Independent verification**: Any party validates without controller gatekeeping

This approach transforms privacy from "trust us" promises into "verify yourself" architecture.

The Problem: Privatized Transparency Infrastructure

Today's privacy ecosystem suffers from three structural failures:

1. Incompatible Standards: Each organization creates custom privacy policies with unique structure, terminology, and disclosure patterns—making comparison impossible and informed consent impractical.

2. Unverifiable Claims: Controllers self-attest compliance through lengthy policies that individuals cannot independently verify. No bilateral proof, no audit trail, no synchronized state.

3. Unscalable Enforcement: Regulators conduct manual audits after harm occurs. Without machine-readable transparency infrastructure, compliance verification cannot scale to millions of controllers.

Result: "Accept All" becomes the only practical option—meaningful consent replaced by legal theater.

The Solution: ISO/IEC 27560-1 Universal Notice Receipt Profile

Convention 108+ as Technical Standard

ISO/IEC 27560-1 implements **Council of Europe Convention 108+** (international data protection treaty, 55+ jurisdictions) as machine-readable transparency infrastructure. Rather than creating a new voluntary code, the profile positions the treaty itself as the normative framework, providing technical operationalization through:

1. Controller Identification Record (CIR): Standardized accountability disclosure published at /.well-known/transparency BEFORE any data collection

2. Universal Notice Receipt: Bilateral proof-of-notice (Two-Factor Notice pattern) where both controller and individual hold synchronized records

3. Notice Event Log: Append-only audit trail of transparency state changes—queryable by individuals and regulators via rights_access_point

4. Digital Transparency Registry: Independent verification infrastructure enabling any party to validate CIR-ID registration and receipt authenticity without accessing personal identifiers

Dual Function:

- **Code of Conduct**: Operationalizes Convention 108+ treaty obligations (Articles 5, 8, 9, 10, 11, 14) as binding transparency requirements
- **Code of Practice**: Provides technical implementation standard for Digital ID trust frameworks (W3C DIDs, eIDAS 2.0, FIDO2) and AI governance transparency (ISO/IEC 42001, EU AI Act)

How It Works: Transparency by Default (TbD) Architecture

Core Principle: Controller-ID First

Transparency by Default (TbD) = Architectural pattern where controller disclosure precedes data collection; transparency is the default state, not an opt-in feature.

Inversion of Traditional Model:

- **Traditional**: User-ID first → "Accept All" → PII collected → privacy policy link
- **TbD**: Controller-ID first → CIR verification → bilateral notice receipt → individual CHOOSES to provide PII

Four-Stage ANCR Exchange

Stage 1 (Notice Receipt):

- Controller presents CIR identification BEFORE requesting PII

- Individual remains ANONYMOUS (no pii_principal_id required)
- Bilateral proof-of-notice via Two-Factor Notice (2FN) pattern
- Universal across all Convention 108+ legal bases (consent, contract, legal obligation, legitimate interest, vital interest, public interest)

Stage 2 (Authorization Receipt):

- Individual returns receipt with explicit authorization
- Granular permissions_bundle specifies scope and purpose
- Synchronized proof of informed authorization
- Notice Event Log updated

Stage 3 (Micro-Notice Credential):

- Cryptographic signature for technical contexts (API authorization, device binding)
- No need to reshare raw receipt
- Enhanced assurance for cross-border or sensitive processing

Stage 4 (Notice Token):

- Individual-controlled portable tokens
- Cross-controller authorization portability
- Agentic AI coordination and consent wallet management

Key Innovation: notice.txt as Universal Baseline

Standard Public Privacy Policy

CIR published at **/.well-known/transparency/notice.txt** replaces custom privacy policies with **standardized baseline** that is:

Machine-Readable:

```
{
  "controller_identity_record_id": "CIR-CA-2024-00123",
```

```
  "controller_name": "Example Data Controller Ltd.",
  "jurisdiction": "CA",
  "lawful_basis": "consent",
  "processing_purposes": ["service_delivery", "analytics"],
  "scope_of_disclosure": "national",
  "rights_access_point": "privacy@example.ca",
  "notice_event_log_url": "https://example.ca/notice-log",
  "codes_of_conduct": "Council of Europe Convention 108+ oper
ationalized via ISO/IEC 27560 Universal Notice Receipt Profil
e v1.0"
}
```

Risk-Proportionate Transparency:

- **Local/Child scope**: Minimal fields (controller-ID, purpose, legal basis)
- **Regional/National scope**: Add processing locations, retention, DPO contact
- **International scope**: Add transfer_mechanism, recipient_jurisdictions, surveillance_risks

Independent Verification: Any party retrieves CIR without authentication—enabling:

- Individuals assess accountability before providing data
- Researchers compare transparency across controllers
- Regulators automate compliance verification
- Digital ID trust frameworks validate controller registration

Convention 108+ Article 11: Surveillance Risk Disclosure

When cross-border transfers involve destination jurisdictions with government access laws (FISA Section 702, Investigatory Powers Act 2016, National Intelligence Law), **material risk disclosure is mandatory**:

surveillance_risks Field:

```
{
  "scope_of_disclosure": "international",
```

```
  "recipient_jurisdictions": ["US"],
  "surveillance_risks": {
    "disclosed": true,
    "jurisdictions": {
      "US": "Foreign Intelligence Surveillance Act Section 70
2 permits government access to data of non-US persons without
notification"
    },
    "legal_frameworks": ["FISA Section 702 (50 U.S.C. § 1881
a)"]
  },
  "transfer_consent_validation": {
    "surveillance_disclosed_at_consent": true
  }
}
```

Legal Basis: Convention 108+ Article 11.3 permits derogations when "provided for by law" and "necessary in a democratic society"—but **transparency about the derogation itself remains mandatory** under Article 8.2.

Implementation Comparison: Traditional vs. Transparency by Default

Aspect	Traditional (Privacy-Preserving)	TbD (Privacy-Enabling)
Primary Identifier	pii_principal_id (required)	controller_identity_record_id (CIR-ID first)
Notice Timing	After PII collection	Before any processing
Transparency Mechanism	Custom privacy policies	Standard notice.txt + Convention 108+
Trust Model	Controller self-attestation	Cryptographic receipts + public registries
Proof	Unilateral controller records	Bilateral receipts (2FN)

Aspect	Traditional (Privacy-Preserving)	TbD (Privacy-Enabling)
Revocation	Requires controller cooperation	Autonomous via Notice Event Log
Enforcement	Manual audits (cannot scale)	Automated verification (scales)
Baseline Policy	None (each controller custom)	Convention 108+ (universal standard)

Co-Regulated Infrastructure: Digital Transparency Registries

Independent Verification Without Controller Gatekeeping

Challenge: Traditional data protection depends on controller cooperation for verification—individuals and regulators cannot independently validate claims.

Solution: Digital Transparency Registries enable **any party** to generate and verify notice receipts using publicly required controller information:

Registry Architecture:

1. **Controller Registration**: Organization registers CIR-ID with supervisory authority (e.g., OPC, ICO, CAI)
2. **Registry Signature**: Authority signs CIR without accessing individual identifiers (blind signature)
3. **Public Verification**: Any party validates receipts against registry's public key
4. **Privacy-Through-Architecture**: Registry never sees pii_principal_id—only CIR-ID

Example Workflow:

1. Controller publishes CIR at /.well-known/transparency
2. Individual retrieves CIR (no authentication)
3. Notice receipt generated using CIR + registry signature
4. Both parties hold synchronized receipt

5. Individual validates receipt against registry's public key

Regulatory Capacity: Supervisory authorities query public registries for compliance patterns:

- Controllers claiming adequacy decisions
- Transfer mechanisms for international scope
- Surveillance risk disclosure compliance
- Automated decision-making transparency

Automated detection without manual investigation—enforcement scales to millions of controllers.

Digital Transparency Privacy Risk Assurance: Three-Dimensional Architecture

Digital Transparency Privacy Risk Assurance operates across three dimensions: **(1) Scope of Disclosure** (local → international processing contexts), **(2) Data Governance Vectors** (Personal Control, Data Protection, Co-Regulation bridged via ANCR Exchange), and **(3) Assurance Levels** (self-assertion → active state verification). Together these create 72 Digital Transparency Control Contexts (3 vectors × 4 levels × 6 legal bases).

Four Assurance Levels

Level 1 (Self-Assertion):

- Controller publishes notice.txt
- Notice receipts optional
- Suitable for local/child scope of disclosure

Level 2 (Registry Verification):

- CIR-ID registered with Digital Transparency Registry
- Independent verification via registry signature
- Suitable for regional/community/national scope

Level 3 (Cryptographic Signatures):

- ANCR Exchange Stage 3 micro-credentials with cryptographic binding
- Suitable for high-risk contexts (cross-border, sensitive categories)

Level 4 (Active State + Physical Verification):

- Real-time CIR hash validation
- Face-to-face liveness assurance for break-the-glass scenarios
- Suitable for critical infrastructure, vital interest, lawful access contexts

---

Why This Matters: Closing Ten Fundamental Gaps

This profile addresses critical limitations in traditional data protection:

1. Identifiers: Controller-ID first (anonymous-by-default) vs. User-ID first (surveillance-by-default)

2. Permissions: Granular permissions_bundle vs. binary tick-box consent

3. Legal Basis: All six Convention 108+ bases vs. consent-only scope

4. Portability: ANCR Exchange Stage 4 portable tokens vs. no cross-controller authorization

5. Verification: Public CIR registries (independently verifiable) vs. controller self-attestation

6. Transparency Standard: Convention 108+ as universal baseline (notice.txt) vs. custom privacy policies per controller

7. Proof: Bilateral receipts (2FN) vs. unilateral controller records

8. Auditability: Notice Event Log (append-only trail) vs. manual investigation after harm

9. Revocation: Immediate via Notice Event Log update vs. controller gatekeeping

10. Enforcement: Automated receipt verification (scales) vs. manual audits (cannot scale)

Core Innovation: By implementing Convention 108+ horizontal transparency requirements as digital public infrastructure through notice.txt, this profile establishes a **universal baseline privacy policy standard** enabling comparison, verification, and enforcement at scale.

For Canadian Regulators: PIPEDA and Law 25 Alignment

PIPEDA Principle 4.1.3 (Accountability): CIR registries provide verifiable accountability infrastructure—controllers demonstrate compliance through public registration before collection begins.

PIPEDA Principle 4.3 (Meaningful Consent): Bilateral receipts with granular permissions_bundle operationalize "meaningful consent" requirement—individual reviews specific authorizations before providing data.

Quebec Law 25 Articles 8, 8.1, 44, 45, 53.1, 65: Enhanced transparency requirements for digital identification technologies, biometric processing, and automated decision-making implemented through:

- CIR publication requirement (Article 8 accountability)
- Scope of disclosure transparency (Article 8.1 proportionality)
- Surveillance risk disclosure (Article 44 cross-border transfers)
- Automated decision notice (Article 45)
- Two-Factor Notice for biometric processing (Article 53.1)
- Notice Event Log for processing records (Article 65)

Federal-Provincial Coordination: CIR registries provide common infrastructure for OPC (federal) and CAI (Quebec) oversight—enabling automated compliance verification without requiring controller gatekeeping.

Commonwealth Leadership Opportunity: Convention 108+ treaty framework (55+ jurisdictions) positions Canada to lead international digital transparency coordination—profile demonstrates how treaty obligations operationalize as enforceable digital public infrastructure.

Digital ID and AI Governance Interoperability

Code of Practice for Trust Frameworks

Controller-ID First Architecture enables trust framework alignment:

W3C Decentralized Identifiers (DIDs):

- CIR-ID functions as organizational DID
- Individual verifies controller accountability before credential issuance
- Anonymous-by-default: DID exchange occurs before PII disclosure

eIDAS 2.0 Digital Identity Wallets:

- Notice receipts stored in wallet alongside credentials
- Cross-border authorization portability via ANCR Exchange Stage 4
- Surveillance risk disclosure for international attribute sharing

FIDO2 Authentication Standards:

- CIR publication required before authenticator registration
- Bilateral notice receipt documents processing purposes for biometric data
- Notice Event Log tracks authentication events

AI System Transparency (ISO/IEC 42001, EU AI Act):

- Automated decision disclosure via CIR processing_purposes
- Model retraining transparency through Notice Event Log
- Cross-border AI deployment documented via scope_of_disclosure
- Explainability mechanisms referenced in rights_access_point

---

Universal Context Applicability

Same transparency infrastructure applies across:

Privacy Context: All six Convention 108+ Article 5 legal bases (consent, contract, legal obligation, legitimate interest, vital interest, public interest)

Safety Context: Product recalls, hazard warnings, emergency notifications

Security Context: Acceptable use policies, incident disclosures, access control

Environment Context: Sustainability reporting, hazardous waste notifications, climate risk

AI System Context: Automated decision disclosure, model deployment transparency, explainability mechanisms

Digital ID Context: Controller-ID first architecture for trust frameworks, biometric processing transparency, cross-border attribute sharing

---

Conformance and Adoption Pathway

Universal Notice Receipt Conformance (Mandatory)

1. **CIR Publication**: Publish Controller Identification Record at /.well-known/transparency BEFORE any processing
2. **Anonymous Accessibility**: Make CIR accessible without authentication
3. **Anonymous-by-Default**: ANCR Exchange Stage 1 SHALL NOT require pii_principal_id
4. **Two-Factor Notice**: Implement 2FN for all contexts requiring bilateral proof
5. **Notice Event Log**: Maintain append-only log accessible via CIR rights_access_point
6. **Scope of Disclosure**: Specify risk category for all processing activities
7. **Convention 108+ Reference**: Use codes_of_conduct field to reference treaty framework
8. **Cross-Border Transparency**: When scope="international", disclose transfer_mechanism, recipient_jurisdictions, surveillance_risks

Adoption Strategy for Regulators

1. **Validate** notice receipt architecture against Convention 108+ transparency requirements
2. **Establish** Digital Transparency Registry infrastructure for CIR publication and verification
3. **Pilot** co-regulated transparency with volunteer controllers across contexts
4. **Integrate** notice receipts into enforcement tools (privacy, safety, security, environment)

5. **Enable** transparency-by-default through public CIR accessibility requirements
6. **Coordinate** with Convention 108+ supervisory authority network for cross-border verification

---

Document Status

Current Version: v1.01 Internal Draft (December 16-22, 2025)

Submission Status:

- v1.0 submitted December 14, 2025 to ISO/IEC JTC 1/SC 27/WG 5 Canadian mirror committee (NON-NORMATIVE submission)
- v1.01 internal draft for stakeholder review and pilot implementation reference (NOT submitted to standards body)

Normative Status: **NOT an international standard**—demonstrator submission showing how transparency infrastructure COULD work if adopted

Conditional Dependencies:

1. ISO/IEC 27560-1 base standard adoption (NOT YET ADOPTED)
2. Convention 108+ entry into force (ratifiable 2026, NOT YET ratified by sufficient signatories)
3. Universal Notice Receipt Profile adoption (depends on #1 and #2)

Author: Mark Lizar, Digital Transparency Lab

License: RF-RAND IPR

Historical Context: Completes Minimum Viable Consent Receipt (MVCR) specification originated by Kantara Initiative (2015), which was adopted as foundation for ISO/IEC TS 27560:2023 and referenced in ISO/IEC 29184:2020 Appendix D. This profile restores original MVCR vision—transparency infrastructure that can be generated independently by individuals, not solely by controllers.

Key Takeaway

ISO/IEC 27560-1 establishes digital public privacy infrastructure where controller identification precedes data collection. By implementing Council of Europe Convention 108+ as machine-readable standard (notice.txt), the profile enables:

- **Independent verification** without controller gatekeeping
- **Universal baseline** replacing incompatible custom privacy policies
- **Enforcement at scale** through automated compliance verification
- **Digital ID interoperability** via Controller-ID first architecture
- **AI governance transparency** through standardized disclosure mechanisms

Tagline: "It's not fair or trustworthy, if it's not Transparent First."

Note: This introduction document provides conceptual overview. For technical implementation details, refer to ISO/IEC 27560-1 Universal Notice Receipt Profile v1.01 specification.