ISO/IEC JTC 1/SC 27 **N 24376**

**ISO/IEC JTC 1/SC 27 "Information security, cybersecurity and privacy protection"**
Secretariat: **DIN**
Committee manager: **Mahmoud Sobhi Mr**

**ISO/IEC CD 27560**

| Document type | Related content | Document date | Expected action |
|---|---|---|---|
| Ballot / Reference document | Ballot: ISO/IEC CD 27560 (restricted access) | 2025-10-28 | **COMMENT/REPLY** by 2025-12-24 |

# ISO/IEC 27560:2025-1 Universal Notice Receipt Profile v1.0

Convention 108+ Article 5 requires legitimate processing with proportionality embedded in context.[3] EU Regulation 2018/1725 Article 4 mandates data minimization—authentication requirements limited to what is necessary for safety purpose.[4][5] EU Regulation 2018/1725 operationalizes Convention 108+ transparency requirements through institutional implementation.[2] GDPR Recital 4 and Article 35(7)(b) require balancing stakeholder rights through proportionate transparency.[6] Quebec Law 25 Articles 8, 8.1, 44, 45, 53.1, and 65 require meaningful consent and enhanced transparency for identification, biometric processing and automated decision-making.[7]

## Document Metadata

**Profile Title**: Universal Notice Receipt Profile for ISO/IEC 27560:2025 - Notice and Consent Receipts for Any Legal Basis

**Version**: 1.0 (Final Submission Draft in progress)

**Base Standard**: ISO/IEC 27560:2025 WD - Structure of Personally Identifiable Information (PII) Processing Records

**Backward Compatibility**: ISO/IEC TS 27560:2023 (see Appendix G)

**Author**: Mark Lizar, Digital Transparency Lab

**License**: RF-RAND IPR License

**Historical Context**: This profile operationalizes **Council of Europe Convention 108+ transparency requirements** as digital public infrastructure for co-regulated transparency. Completes the **MVCR - Open Notice** purpose co-invented in 2013 by Phil Pearce and Reuben Binns, and formalized as the Minimum Viable Consent Receipt (MVCR v0.9) specification by the Kantara Initiative in 2015. The MVCR work was adopted as the foundation for ISO/IEC TS 27560:2023 and referenced in ISO/IEC 29184:2020 Appendix D. Rather than creating a new code of conduct, this profile implements Convention 108+ Articles 5, 8, 9, 10, and 14 as operational transparency infrastructure supporting all six legal bases through bilateral notice receipts, public Controller Identification Records, and Notice Event Logs.

**Acknowledgments**: This profile builds upon the foundational **MVCR - Open Notice** architecture co-invented with Valentino Spataro, Phil Pearce and Reuben Binns (2013), facilitated by Andrew Hughs and Colin Wallis and the MVCR v0.9 specification developed by the Kantara Initiative Consent & Information Sharing Work Group (2015). Contributors to the MVCR work include: John Wunderlich, Mary Hodder, Reuben Binns,  Renee Lloyd, Iain Henderson, Joe Andrieu, Tim Reiniger, Eve Maler, Joni Brennan, Joss Langford, Joel Geddes and Sal D'Agostino.  **In memory of Nick Givotovsky** 🕊️, whose contributions inspired the MVCR vision that continues to shape digital transparency infrastructure.

---

# Document Metadata

# Executive Summary

**Problem**: Current data protection frameworks were designed for analog contexts—face-to-face consent with inherent controller visibility and physical observation of privacy risks. Digital identification inverts this: controllers infer identities instantly across borders before individuals know who is collecting their data, yet privacy law still assumes accountability happens "at collection."

**Solution**: The Universal Notice Receipt Profile inverts data protection architecture by putting **Controller-ID first, not User-ID first**. Before any processing or identifier inference begins, controllers publish a Controller Identification Record (CIR) at a public location—enabling individuals to verify accountability before providing data. Both parties hold synchronized bilateral receipts, creating cryptographic proof of transparency state.

**Key Innovation**: This profile completes the original Minimum Viable Consent Receipt (MVCR) vision through **co-regulated transparency infrastructure**—notice receipts can be generated independently by individuals using publicly required controller information, not solely by controllers after obtaining permission. This enables transparency-by-default through Convention 108+ horizontal requirements operationalized as digital public infrastructure. Implemented as code of conduct.

## What Changes

**Traditional Data Protection** (User-ID First):

1. Individual visits website → "Accept All" popup → provides email/password
2. Controller NOW has PII BEFORE meaningful notice
3. Privacy policy link (lengthy, unread, incompatible per controller)
4. Unilateral controller record—individual has no proof
5. Revocation requires controller cooperation (30-day response)
6. Manual audits—cannot scale enforcement

**Universal Notice Receipt** (Controller-ID First):

1. Controller publishes CIR at /.well-known/transparency BEFORE any interaction
2. Individual retrieves CIR and generates notice receipt—remains ANONYMOUS
3. Standardized notice.txt—Convention 108+ as universal baseline privacy policy
4. Bilateral receipts—both parties hold synchronized proof via Two-Factor Notice (2FN)
5. Autonomous withdrawal—Notice Event Log updates enable real-time revocation
6. Automated enforcement—public CIR registries scale regulatory verification

## Four-Stage ANCR Exchange

**Stage 1 (Notice Receipt)**: Controller presents CIR identification **before** requesting PII—enabling anonymous-by-default engagement with bilateral proof

**Stage 2 (Authorization Receipt)**: Individual returns receipt with explicit authorization (consent, contract, legal obligation, etc.)—creating synchronized proof of informed consent

**Stage 3 (Micro Notice Credential)**: Authorization becomes cryptographically verifiable credential for API/device authorization without resharing raw receipt

**Stage 4 (Consent Token)**: Individual-controlled portable tokens enable cross-controller consent portability, agentic AI coordination, and authorization wallet management

## Why This Matters for Canada

**PIPEDA Alignment**: Profile implements PIPEDA Principle 4.1.3 (accountability) and 4.3 (meaningful consent) through verifiable infrastructure—controllers demonstrate accountability through public CIR registries before collection begins

**Quebec Law 25 Compliance**: Addresses Law 25 Articles 8, 8.1, 44, 45, 53.1, and 65 requirements for meaningful consent and enhanced transparency for digital identification technologies, biometric processing, and automated decision-making

**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

## Convention 108+ as Digital Public Infrastructure

Rather than creating a new code of conduct, this profile positions **Council of Europe Convention 108+** as the normative legal framework for digital identification transparency:

- **Article 8 (Transparency)**: CIR publication and notice receipts implement controller identification requirements
- **Article 9 (Proportionality)**: Risk-based scope of disclosure determines transparency obligations (local/child → international)
- **Article 10 (Accountability)**: Notice Event Logs provide append-only register of processing operations
- **Article 14 (Cross-Border Transfers)**: Surveillance risk disclosure and recipient jurisdiction fields enable informed consent for international transfers

**Profile adds**: Technical operationalization (CIR infrastructure, bilateral receipts, Notice Event Logs) and risk-proportionate transparency through four TATA (Transparency and Trust Assurance) levels

## What This Profile Does

**MANDATORY (Universal Notice Receipt Conformance)**:

- Publish Controller Identification Record at public location BEFORE processing
- Implement Two-Factor Notice (2FN) for bilateral proof
- Maintain Notice Event Log accessible via CIR rights access point
- Specify scope of disclosure for risk-proportionate transparency
- Support notice receipts across privacy, safety, security, environment contexts
- Use anonymous-by-default architecture (no pii_principal_id in Stage 1)

**OPTIONAL (Authorization Exchange Extensions)**:

- Stage 2 authorization exchange for consent/contract contexts

- Stage 3 cryptographic credentials for API/device authorization
- Stage 4 portable consent tokens for cross-controller portability

## What This Profile Does NOT Do

- **Not operational lawful interception infrastructure**: Does not replace ETSI LI standards for communications interception
- **Not new legal basis**: Implements existing Convention 108+ requirements through verifiable infrastructure
- **Not creating new law**: Operationalizes existing transparency obligations as digital public infrastructure
- **Not controller compliance tool**: Regulatory capacity infrastructure for enforcement at scale (privacy-enabling, not privacy-preserving)

## Eight Derivative Digital Transparency Controls

This profile operationalizes **eight derivative digital transparency controls** required by Convention 108+ when digital identification technologies are deployed (see Appendix H for complete analysis):

| Privacy Right / Control | Legal Basis Context | Convention 108+ Article | v1.0 Status |
|---|---|---|---|
| **Derivative Digital Transparency Controls** | | | |
| Controller-ID Before Inference | All Bases | Article 8 + 9 | ✅ Mandatory |
| Scope of Disclosure Transparency | All Bases | Article 9 + 14 | ✅ Mandatory |
| Digital Surveillance Risk Disclosure | All Bases (cross-border) | Article 14.2 + 11.3 | ✅ Mandatory |
| Bilateral Notice Proof (2FN) | All Bases | Article 8 + 12 | ✅ Mandatory |
| Notice Event Log Access | All Bases | Article 8 + 9 + EU 2018/1725 Art. 88 | ✅ Mandatory |
| Autonomous Consent Withdrawal | Consent | Article 9 + 8 | ✅ Mandatory |
| Active State Transparency | All Bases | Article 8 + 9 | ⚠️ Optional (TATA L4) |
| Notice of Derogation to Digital Surveillance Rights | Consent (cross-border) | Article 11.3 + 8 + 5.2 | ✅ Mandatory |
| **Traditional Data Protection Rights** | | | |
| Right to Be Informed | All Bases | Article 8 | ✅ Supported |
| Right to Access | All Bases | Article 9 | ✅ Supported |
| Right to Rectification | All Bases | Article 9 | ✅ Supported |
| Right to Erasure | Consent | Article 9 | ✅ Supported |

| Privacy Right / Control | Legal Basis Context | Convention 108+ Article | v1.0 Status |
|---|---|---|---|
| Right to Withdraw Consent | Consent | Article 5 | ✅ Supported |
| Right to Data Portability | Consent | Article 9 | ✅ Supported |

**Key Distinction**: The eight derivative controls are **proportionate extensions** of traditional rights required when digital identification technologies are deployed. They are not new rights—they operationalize existing Convention 108+ transparency obligations for digital contexts where controllers can identify individuals instantly across borders before collection begins.

## Implementation Impact

**For Controllers**:

- Register CIR with authoritative source (e.g., OPC, CAI, provincial commissioners)
- Publish standardized notice.txt at /.well-known/transparency
- Generate bilateral notice receipts for all processing contexts
- Maintain queryable Notice Event Log

**For Individuals**:

- Generate notice receipts independently using public CIR
- Remain anonymous until choosing to authorize (Stage 2)
- Exercise rights via CIR rights access point
- Portable consent tokens enable cross-controller authorization

**For Regulators**:

- Automated verification through public CIR registries
- Receipt validation scales enforcement without controller cooperation
- Cross-border coordination through Convention 108+ supervisory authority network
- Notice Event Log queries enable continuous oversight

## Cross-Border Transfer Transparency

Profile addresses Schrems II gaps through enforceable surveillance risk disclosure:

- **transfer_mechanism**: Documents legal basis for cross-border transfer (consent, adequacy, SCC, BCR)
- **recipient_jurisdictions**: ISO 3166-1 alpha-2 country codes for destination transparency
- **surveillance_risks**: Explicit disclosure of FISA 702, IPA 2016, National Intelligence Law surveillance frameworks
- **rights_derogations**: Which Convention 108+ Article 9 rights are suspended under destination jurisdiction national security laws
- **transfer_consent_validation**: Proves individual was informed of surveillance risks BEFORE consent

## Universal Context Applicability

Same base requirements apply across contexts beyond privacy:

- **Safety**: Product recalls, hazard warnings, emergency notifications
- **Security**: Acceptable use policies, incident disclosures, access control
- **Environment**: Sustainability reporting, hazardous waste notifications, climate risk
- **AI Systems**: Automated decision disclosure, model retraining transparency (Appendix J—informative)

## Standards Alignment

- **Base Standard**: ISO/IEC 27560:2025 WD (field-level compatible with Section 6.5)
- **Backward Compatible**: ISO/IEC TS 27560:2023 (see Appendix G for migration guidance)
- **Normative Framework**: Convention 108+ (not GDPR—treaty provides universal baseline)
- **Operational Reference**: EU Regulation 2018/1725 (best-practice implementation of Convention 108+)
- **Semantic Interoperability**: W3C Data Privacy Vocabulary (DPV) alignment for privacy contexts
- **Related Development**: ISO/IEC 27568 (Digital Twins), ISO/IEC 27566 (Age Assurance), ISO/IEC 27091 (Gen AI), ISO/IEC 27701 (PIMS), IEEE P7012 (Machine Readable Privacy Terms)

## Submission Status

**Version**: 1.0 Final Submission Draft

**Target**: Canadian mirror committee for ISO/IEC JTC 1/SC 27/WG 5

**Author**: Mark Lizar, Digital Transparency Lab

**License**: RF-RAND IPR License

**Conformance Levels**: Universal Notice Receipt (mandatory) | Authorization Exchange (optional) | Full Protocol (optional Stage 3-4)

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

---

# PART 1: CO-REGULATED NOTICE RECEIPT ARCHITECTURE

## Controller-ID First Infrastructure Enabling Glass Boxed Transparency Based Governance Model

### Section 1: Scope

**1.1 Profile Objectives**

**Primary Innovation: Four-Stage ANCR (Anchored Notice and Consent Receipt) Authorization Exchange**

This profile demonstrates digital consent through a four-stage bilateral receipt exchange that inverts traditional data protection architecture:

**ANCR Exchange Stage 1: Notice Receipt (or privacy receipt)**: Controller presents identification linked to the Controller Identification Record BEFORE assigning an identifier or requesting any PII — enabling trust capable interaction with anonymous-by-default engagement where individuals verify controller accountability before providing data.

> **Editorial Note**: The controller-id can be used as a pii_principal_identifier by the PII Principal, with permission in a consent flow.

**ANCR Exchange Stage 2: Consent Notice Receipt**: Individual returns Stage 1 receipt with explicit authorization — creating bilateral proof of informed consent, contract acceptance, or a required policy acknowledgment

**ANCR Exchange Stage 3: Micro Notice Credential**: Authorization becomes cryptographically verifiable credential — enabling API authorization, device binding, and remote verification without resharing raw receipt

**ANCR Exchange Stage 4: Consent Token**: Individual adds micro-credential to a notice receipt to anchor the authorization for a secondary purpose of use, utilising the controller id record (CIR) as a personal identifier (DID) — enabling cross-controller consent portability, agentic AI coordination, and authorization wallet management without exposing or transfering PII across jurisdictions.

**ANCR Exchange Stage 4: Consent Token**: Individual anchors authorization to personal identifier (DID) — enabling cross-controller consent portability, agentic AI coordination, and authorization wallet management

---

## Visual Flow: Four-Stage ANCR Authorization Exchange with the Authority of Consent

**Stage 1: Anonymous Notice Receipt (Controller-ID First)**

```
 ┌──────────────────────────────────────────────────────────────────────
──────────┐
 │ BEFORE ANY PII COLLECTION OR PROCESSING                    │
 └──────────────────────────────────────────────────────────────────────
──────────┘

   CONTROLLER                    INDIVIDUAL
   ┌───────────┐                  ┌───────────┐
   │     │           │     │
   │  CIR  │──────────-───────────→ │ Reviews │
   │ notice. │  1. Present CIR     │  CIR  │
   │  txt  │   (public)     │     │
   │     │           │     │
   └───────────┘                  └───────────┘
     │                │
     │                │
     │ ←──────────────────────────────── │
     │  2. Generate Notice Receipt   │
     │    (bilateral proof)     │
     ▼                ▼
   ┌───────────┐                  ┌───────────┐
   │ Receipt │               │ Receipt │
   │  Copy  │               │  Copy  │
   └───────────┘                  └───────────┘

   NO pii_principal_id required
   Individual remains ANONYMOUS
```

**Key Fields**: `controller_identity_record_id`, `receipt_id`, `notice_type`, `scope_of_disclosure`, `two_factor_notice_indicator: true`, **ABSENT**: `pii_principal_id`

**Stage 2: Authorization Receipt (Explicit Consent with Bilateral Proof)**

```
INDIVIDUAL                    CONTROLLER

┌─────────┐                   ┌─────────┐
│ Reviews │                   │ Awaits  │
│ Stage 1 │                   │  Auth   │
│ Receipt │                   │         │
└─────────┘                   └─────────┘
     │                              │
     │──────────────────────────────→│
     │  3. Return Receipt with       │
     │     authorization_type        │
     │     (consent_granted)         │
     │     + permissions_bundle      │
     │     + OPTIONAL pii_principal_id │
     │                              │
     │←──────────────────────────────│
     │  4. Update Notice Event Log   │
     │     Both hold authorized      │
     │     receipt copy              │
     ▼                              ▼
┌─────────┐                   ┌─────────┐
│  Auth   │                   │  Auth   │
│ Receipt │                   │ Receipt │
│  Copy   │                   │  Copy   │
└─────────┘                   └─────────┘

Bilateral proof of informed consent
Notice Event Log updated
```

**Fields Added:** `authorization_type`, `permissions_bundle`, `pii_principal_id` (optional), `consent_timestamp`

**Stage 3: Micro Notice Credential (Cryptographic Verification)**

```
INDIVIDUAL                    API / DEVICE

┌─────────┐                   ┌─────────┐
│  AuthC  │                   │ Service │
│ Receipt │                   │ Requires│
│         │                   │  Auth   │
└─────────┘                   └─────────┘
     │                              │
     │──────────────────────────────→│
     │  5. Present credential with   │
     │     cryptographic_signature   │
     │     + credential_binding      │
     │     + technical_permissions   │
     │                              │
```

```
    │ ←──────────────────────────────────│
    │  6. Verify signature against    │
    │     Controller's public key     │
    │     (from CIR registry)        │
    │                              │
    │  ✓ Authorization confirmed     │
    ▼                              ▼
 ┌──────────┐                 ┌──────────┐
 │ Granted  │                 │ Access   │
 │ Access   │                 │ Granted  │
 └──────────┘                 └──────────┘

No need to reshare full receipt
Cryptographic proof sufficient
```

**Fields Added:** `cryptographic_signature`, `credential_binding`, `technical_permissions_scope`, `validity_period`

**Stage 4: Portable Consent Token (Individual-Controlled Cross-Controller Authorization)**

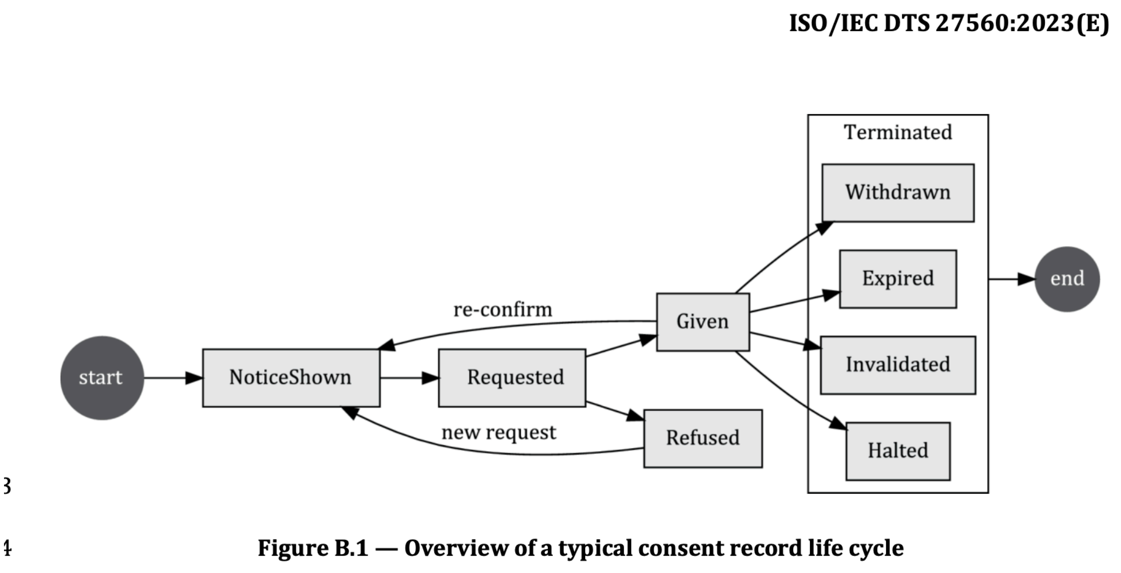
```
INDIVIDUAL                THIRD-PARTY CONTROLLER

 ┌──────────┐                 ┌──────────┐
 │ Consent  │                 │   New    │
 │  Wallet  │                 │ Service  │
 │          │                 │          │
 └──────────┘                 └──────────┘
    │                              │
    │ ──────────────────────────────→ │
    │  7. Present portable token      │
    │     anchored to principal_id    │
    │     (DID, public key)           │
    │     + cross_controller_metadata │
    │                              │
    │  8. Verify token:             │
    │     - Lookup original CIR-ID    │
    │     - Validate signature       │
    │     - Check Notice Event Log    │
    │     - Confirm portability_scope │
    │                              │
    │ ←──────────────────────────────────│
    │  ✓ Consent honored without     │
    │    re-authorization            │
    ▼                              ▼
 ┌──────────┐                 ┌──────────┐
 │ Retains  │                 │ Honors   │
 │ Control  │                 │  Token   │
 └──────────┘                 └──────────┘
```

```
Cross-controller portability
Individual controls authorization distribution
```

**Fields Added:** `principal_anchor` (DID | public key | wallet address), `token_claims` , `cross_controller_metadata` , `portability_scope`

## Architectural Comparison: Traditional vs. ANCR

### Traditional Data Protection Flow:



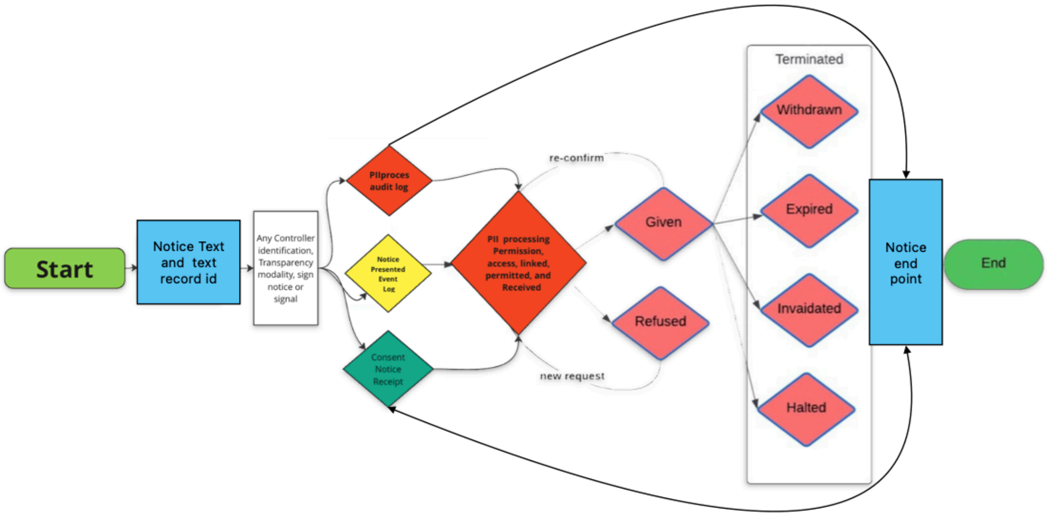
ISO/IEC DTS 27560:2023(E)

**Figure B.1 — Overview of a typical consent record life cycle**

```
1. Individual visits website
2. "Accept All" popup (no real choice)
3. Individual provides email/password
4. Controller NOW has PII BEFORE notice
5. Privacy policy link (lengthy, unread)
6. No bilateral proof
7. No independent verification
8. Revocation requires controller cooperation
```

### ANCR Digital Consent Flow:

## ISO/IEC 27560 -1 :2025 Universal Receipt Profile v.1
## Co-Regulated Notice Even Logging


Start
Notice Text and text record id
Any Controller identification, Transparency modality, sign notice or signal
PIIproces audit log
Notice Presented Event Log
Consent Notice Receipt
PII processing Permission, access, linked, permitted, and Received
re-confirm
new request
Given
Refused
Terminated
Withdrawn
Expired
Invaidated
Halted
Notice end point
End

1. Controller publishes CIR BEFORE interaction
2. Individual retrieves CIR (verifies accountability)
3. Stage 1 Notice Receipt (bilateral proof)
4. Individual remains ANONYMOUS
5. Individual reviews permissions_bundle
6. Individual CHOOSES to authorize (Stage 2)
7. Both parties hold synchronized receipt
8. Notice Event Log tracks state changes
9. Portable consent token (Stage 4)
10. Cross-controller portability

**Key Innovation**: ANCR inverts traditional data protection by putting **Controller-ID first** (not User-ID first), enabling accountability to precede collection, bilateral proof instead of unilateral records, independent verification instead of self-attestation, and automated enforcement instead of manual audits.

**Core Objectives:**

**What This Profile Does NOT Do:**

- **Not operational security for lawful interception**: Does not replace ETSI LI standards or government surveillance infrastructure for communications interception

**Key Innovation**: ANCR inverts traditional data protection by putting **Controller-ID first** (not User-ID first), enabling accountability to precede collection, bilateral proof instead of unilateral records, independent verification instead of self-attestation, and automated enforcement instead of manual audits.

**Legal Framework Integration:**

This profile extends ISO/IEC 27560:2025 by operationalizing **Council of Europe Convention 108+** as the normative code of conduct through the base standard's `codes_of_conduct` field (clause 6.3.4.20). Rather than creating a new voluntary code, this profile positions Convention 108+ as the authoritative international treaty framework, with this profile serving as the technical implementation specification for digital identification transparency.

**Positioning:**

- **Convention 108+** = Normative legal framework (treaty obligations, Articles 5, 8, 9, 10, 14)
- **This profile** = Technical operationalization (CIR infrastructure, notice receipts, bilateral proof mechanisms)
- **codes_of_conduct field** = Linkage mechanism enabling controllers to reference treaty compliance

See Section 10 for complete Convention 108+ article mapping.

**Core Objectives:**

**What This Profile Does NOT Do:**

- **Not operational security for lawful interception**: Does not replace ETSI LI standards
- **Not data access protocol**: Does not define how authorities intercept communications or access stored data operationally
- **Not enforcement execution**: Provides transparency for enforcement oversight, not mechanisms for seizure, blocking, or takedown operations

This profile operationalizes **regulatory capacity infrastructure** for lawful oversight through transparent, front-door access—not operational lawful interception through secret, back-door access. It enables glass-box regulatory verification without replacing law enforcement technical access protocols.

**Core Objectives:**

- Complete the original MVCR purpose through co-regulated transparency infrastructure to scale specified consent online referred to as digital consent
- Restores original MVCR function: notice receipts can be generated independently by individuals using publicly required controller information, not solely by controllers after obtaining permission
- Demonstrate digital consent as Four-Stage interaction from digital transparency by default as, Default transparency with Controller-ID → Authorization → Credential → Portable Consent Token
- Extend ISO/IEC 27560:2025 with notice-first architecture supporting all Convention 108+ lawful bases through Controller Identification Record (CIR) presentation before processing
- Enable co-regulated transparency infrastructure where notice and consent receipts can be generated independently using publicly required controller information

- Support transparency-by-default through bilateral ANCR (both controller and individual hold synchronized proof of notice and evidence of valid consent state)
- Provide digital public infrastructure for ANCR exchange across all legal bases and contexts (privacy, safety, security, environment)
- Enable ANCR Exchange Stage 1 notice receipt to validate PII Processing records as consent records as an ANCR Exchange Stage 2 exchange (previously called consent notice receipt in ISO/IEC 29184, consent receipt when first adopted from MVCR(Minimum Viable Consent Receipt), also known as privacy notice receipt, or privacy policy receipt as it was originally generated from a privacy policy)

> **Editor's Note**: ANCR Exchange Stage 1 (Notice Receipt) can be generated even when notice is missing, enabling bilateral accountability and transparency restoration in contexts where notification was not previously provided.

### 1.2 Scope: Digital Privacy Across All Legal Bases

Notice and consent receipts defined in this profile apply to PII processing under any Convention 108+ lawful basis:

- **Consent**: Freely given, specific, informed agreement
- **Contract**: Processing necessary for contract performance
- **Legal Obligation**: Processing required by law
- **Legitimate Interest**: Processing based on legitimate interests with balancing test
- **Vital Interest**: Processing necessary to protect vital interests (life, health, safety)
- **Public Interest**: Processing for public interest tasks (research, journalism, archiving)

All legal bases share base requirements: controller identification before notice, and a notice event log, and capable of bilateral receipt generation, audit trail maintenance, and rights access point provision.

### 1.3 Profile Boundaries

- Defines ANCR Exchange Stage 1 (Notice Receipt) as mandatory base implementation
- Part 2 (Authorization Exchange Protocol) provides optional extensions for consent portability and authorization coordination
- Maintains field-level compatibility with ISO/IEC 27560:2025 Section 6.5
- Demonstrates co-regulated infrastructure: receipts can be generated independently of controller using publicly available CIR information

### 1.4 Terminology: Notice and Consent Receipts

**Notice Receipt** (this profile): Bilateral record documenting controller notification for PII processing under any legal basis

**Consent Notice Receipt** (backward compatible with ISO/IEC TS 27560:2023): Notice receipt with authorization_type="consent_granted"

**Privacy Receipt** (ISO/IEC 27560:2025): Synonym for notice receipt in PII processing contexts

**Notice Type Categories**:

- **Notification**: Privacy notice presentation requiring acknowledgment
- **Disclosure**: Material information of risk relative to ‘scope of disclosure’ requiring explicit acknowledgment (e.g., material change, data breach)
- **Statement**: Notice statement documenting processing activity or controller assertion
- **Policy**: Privacy policy or terms governing PII processing
- **Signal**: Machine-readable preference or control signal (e.g., Do Not Track, Global Privacy Control)

**Authorization Type by Legal Basis** (ANCR Exchange Stage 2):

- **consent_granted**: Agreement to processing under consent legal basis
- **contract_accepted**: Agreement to contractual terms requiring PII processing
- **legal_obligation_acknowledged**: Acknowledgment of processing under legal obligation
- **legitimate_interest_notified**: Notification of legitimate interest processing (with opt-out)
- **vital_interest_notified**: Notification of vital interest processing (emergency contexts)
- **public_interest_notified**: Notification of public interest processing

---

## Section 2: Normative References

### 2.1 Primary Normative References

- **Council of Europe Convention 108+** — Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data (ratifiable international treaty, 55+ jurisdictions)
    - Article 5: Legitimacy and proportionality of data processing
    - Article 8(2): Transparent processing and information to data subjects (a receipt and notice event log shall be required for transborder flows)
    - Article 9: Rights of the data subject (access, rectification, erasure)
    - Article 10: Additional obligations (records of processing operations)
    - Article 14: Transborder flows of personal data (adequate safeguards)
- **ISO/IEC 27560:2025 WD** — Structure of Personally Identifiable Information (PII) Processing Records (base technical standard)
- **ISO/IEC 29100:2011** — Privacy framework (Principle 7: Transparency)

### 2.2 Operational Implementation References

- **EU Regulation 2018/1725** — Protection of natural persons with regard to the processing of personal data by Union institutions, bodies, offices and agencies (best-practice operational implementation of Convention 108+ for institutional transparency)
- Article 15: Information to be provided where personal data are collected

- Article 31: Records of processing activities, including public central register (Article 31(5))
- Article 68: Transfers of personal data to third countries or international organisations

> **Editor's Note**: Articles 15, 31, and 68 referenced above are from EU Regulation 2018/1725, which provides operational implementation of Convention 108+ transparency requirements for EU institutions. Article 31(5) specifically mandates a public central register of processing activities—a key precedent for the Controller Identification Record (CIR) infrastructure defined in this profile.

- **W3C Data Privacy Vocabulary (DPV)** (semantic governance interoperability)

**2.3 Non-Normative References**

- **GDPR (EU 2016/679)** — General Data Protection Regulation (jurisdictional example of Convention 108+ implementation for EU/EEA)
- **ISO/IEC 29184:2020** — Online privacy notices and consent (Appendix D references Kantara MVCR work)

**2.4 Legal References**

[1] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+), 2018

[2] European Union, Regulation (EU) 2018/1725 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies, 2018

[3] Council of Europe, Convention 108+, Article 5: Legitimacy and proportionality of data processing

[4] European Union, Regulation (EU) 2018/1725, Article 4: Lawfulness of processing

[5] European Union, Regulation (EU) 2018/1725, Article 4(1)(c): Data minimization principle

[6] European Union, Regulation (EU) 2016/679 (GDPR), Recital 4 and Article 35(7)(b): Balancing of rights through proportionate transparency

[7] Quebec, Act to modernize legislative provisions as regards the protection of personal information (Law 25), 2021, c. 25, Articles 8, 8.1, 44, 45, 53.1, 65

[8] Convention 108+, Article 8(2): Transparent processing and information to data subjects

[9] Convention 108+, Article 9: Rights of the data subject

> **Note on ISO/IEC 29184:2020 Exclusion from Normative References**: This standard is not free and open to access, which makes it incompatible with co-regulated transparency infrastructure requirements. Digital public infrastructure for transparency-by-default requires that all normative standards be publicly accessible to enable independent notice receipt generation by individuals, third-party verification services, and regulatory oversight at scale. Additionally, **ISO/IEC 29184:2020 is not required as this profile uses Convention 108+ as the authoritative international treaty framework** for data protection transparency requirements. ISO/IEC 29184:2020 is acknowledged here for its historical contribution (Appendix D references the Kantara MVCR work that this profile completes), but cannot be

> normative for a transparency infrastructure designed to be universally accessible and authoritative.

## Section 3: Terms and Definitions

For purposes of this profile, terms and definitions from ISO/IEC 27560:2025, ISO/IEC 29100, and Convention 108+ apply, along with:

**3.1 Controller Identification Record (CIR)**

Structured grouping of publicly required controller information (base standard party fields scoped to Controller role), enabling independent notice receipt generation and privacy state transparency

**3.2 Controller Identification Record Identifier (CIR-ID)**

Unique public reference enabling registry verification and cross-jurisdictional lookup

**3.3 Notice Receipt**

Universal bilateral record documenting controller notification for safety, security, and digital privacy contexts; both controller and individual hold synchronized proof of notice

**3.4 Two-Factor Notice (2FN)**

Pattern where controller presents notice AND generates proof-of-notice record that can be twinned as a receipt to be held  by both parties (also: Two-Factor Record of Notice Activity)

**3.5 Notice Record**

Controller-maintained record of notice issuance (superset of "PII processing record")

**3.6 Scope of Disclosure**

Risk categorization determining proportionate transparency obligations (child, youth, vulnerable, community, regional, national, international)

**3.7 Notice Event Log**

Append-only log of notice receipt state changes, authorization grants, material changes to active purpose and state of data control

**3.8 ANCR Exchange Stage 1 (Notice Receipt)**

Notice receipt issued before identification inference, processing, and interaction, enabling anonymous-by-default engagement

**3.9 Anonymous-by-default**

Architecture in which the individual remains unidentified to controller unless choosing to link and self-disclose identity for identification permissions

**3.10 Notice-first architecture**

Controller identification precedes individual identification to  validate legal basis

**3.11 Co-regulated transparency infrastructure**

System enabling independent notice receipt generation using publicly required controller information, supporting transparency-by-default without dependency on controller participation

**3.12 Transparency-by-default**

Architectural principle where controller accountability information is publicly accessible, enabling bilateral notice receipt generation before inference, any processing or interaction begins

**3.13 Sharing vs Disclosure**

- Sharing: Transfer of personal information by PII Principal
- Disclosure: Transfer of personal information by Controller to third-party controller or processor

**3.14 Digital Risk**

Online  safety, security, and privacy risk determined by scope of disclosure , context and disclosure scope of the surveillance technologies used. For example. each identifier disclosure in a RTB (real time bidding) system would be considered a new digital risk vector

**3.15 Macro Data**

Externally inferred attributes utilized as identifiers

**3.16 Micro Data**

Personally derived attributes with explicit permission to be linked to identifiers (e.g., device ID)

**3.17 Identification vs Identity**

- **Digital Identification**: Surveillance practice where controllers infer or assign identifiers to people (top-down, controller-controlled)
- **Digital Identity**: In a co-regulated environment. sousveillance practice is required where individuals self-define and control their own identifiers, binding them to the CIR they choose to interact with (bottom-up, individual-controlled)

> **Editor's Note**: This distinction is fundamental to the co-regulated transparency model. Traditional data protection standards use "identification" in the surveillance paradigm (controller identifies individual). This profile operates in the identity paradigm (individual controls identifiers and anchors them to controller records).

**3.18 Privacy-Enabling**

Individual-centric data control where individuals control their own data and identifiers without requiring corporate identification or permission. Privacy-enabling architecture gives individuals the power to decide what to share, with whom, and under what conditions—before any processing begins. This paradigm positions transparency as prerequisite to processing, enabling individuals to assess risk and make informed decisions with full autonomy.

**3.19 Privacy-Preserving**

Controller-centric data protection where companies protect data better on behalf of individuals after collection has occurred. Privacy-preserving approaches focus on organizational safeguards, technical protections, and compliance mechanisms that operate after individuals have already provided data and identifiers to controllers. This paradigm treats transparency as post-collection accountability.

> **Editor's Note**: The distinction between privacy-enabling and privacy-preserving reflects a fundamental architectural choice. This profile is regulatory capacity infrastructure for enforcement at scale (privacy-enabling), not compliance tools for companies (privacy-preserving). The CIR infrastructure enables individuals to control whether collection happens, not merely how companies protect data they have already collected.

> **Editor's Note**: This distinction is fundamental to the co-regulated transparency model. Traditional data protection standards use "identification" in the surveillance paradigm (controller identifies individual). This profile operates in the identity paradigm (individual controls identifiers and chooses to anchor them to controller identified records) and is natively conformant and complint for corss border digital identification.

### 3.18 PII Principal

Individual who is interacting with a service using a device, who may or may not be the data subject of the personal data being processed or collected. This interacting individual contributes session specific identifiers, in addition to personal data referred to as personally identifiable information—specifically, attributes and/or identifiers stored as data in a record field.

> **Editor's Note**: The distinction between PII Principal (interacting individual) and Data Subject (individual whose data is protected) is required for co-regulatory model granularity. The PII Principal may interact on behalf of a Data Subject, or may interact anonymously without being a Data Subject at all until choosing to link identifiers.

### 3.19 Data Subject

Individual whose personal data is being protected by a data controller, and is beneficiary of privacy rights and permission controls. The data subject may or may not be the PII Principal interacting with a PII Controller.

### 3.20 Consent (Legal Basis)

The lawful basis under Convention 108+ and privacy law that grants legal authority for processing and transfer of personally identifiable information. Consent is a human (PII Principle) authority to make a decision with legal consequence, distinct from technical permission.

> **Editor's Note**: In the co-regulatory model, consent provides the legal authority that enables technical permissions. This is not a technical checkbox or opt-in mechanism—it is the legal basis that makes identifier processing and disclosure lawful.

### 3.21 Permissions (Technical Access Controls)

Technical system access controls that specify what operations are authorized on which data captured. In the co-regulatory model, permissions are encoded in the `permissions_bundle` field and operationalize the authority of consent into granular, role-based access controls.

**Permissions Structure**:

- **Identifier Permissions**: Authorization to collect, link, or process specific identifiers (e.g., email, device ID, IP address)
- **Processing Permissions**: Authorization for specific operations (read, write, update, delete, share, analyze)
- **Purpose Permissions**: Authorization tied to specific processing purposes (service delivery, analytics, marketing)
- **Disclosure Permissions**: Authorization for sharing with specific third parties or categories

> **Editor's Note**: The permissions_bundle bridges legal consent and technical enforcement. When an individual provides consent (legal basis), the permissions_bundle documents exactly what technical operations that consent authorizes. Without consent, permissions cannot be lawfully exercised for PII processing.

### 3.22 Shared Preferences (User-Controlled Settings)

Individual-controlled configuration settings that operate within the scope of granted consent and permissions. Shared preferences express how an individual chooses to exercise authorized permissions across services, contexts, or controllers.

**Shared Preferences Characteristics**:

- **Scope-Limited**: Can only configure options within already-granted permissions
- **Cross-Controller**: May be portable across controllers (e.g., "always decline marketing," "prefer minimal data collection")
- **Revocable**: Can be changed without requiring new consent if within existing permission scope
- **Non-Binding for New Processing**: Cannot authorize new processing that exceeds existing permissions

**Examples**:

- Privacy preference: "Minimize data collection where optional" (applies within existing consent)
- Communication preference: "Email preferred over SMS" (applies to already-authorized contact methods)
- Disclosure preference:  "Share with research partners" (only if secondary purpose consent includes research)

> **Editor's Note**: The distinction between consent, permissions, and shared preferences is critical for the co-regulatory model:

> - **Consent** = Legal basis (requires legal notice, free choice, withdrawal right controlled by individual)

> - **Permissions** = Technical implementation and enforcement of consent (what systems are authorized to do)

> - **Shared Preferences** = PII principal choices within permission scope (how individuals exercise their control)

> Traditional data protection conflates these concepts, treating online preference checkboxes as "consent." This profile separates them: consent is the legal basis used to grant permissions; permissions enable processing; shared preferences configure how that processing operates within authorized scope providing for  direct permissioning and autonomous consent withdrawl

### 3.21 Permissions (Technical Access Controls)

Technical system access controls that specify what operations are authorized on which data captured. In the co-regulatory model, permissions are encoded in the `permissions_bundle` field and operationalize the authority of consent into granular, role-based access controls.

**Permissions Structure**:

- **Identifier Permissions**: Authorization to collect, link, or process specific identifiers (e.g., email, device ID, IP address)
- **Processing Permissions**: Authorization for specific operations (read, write, update, delete, share, analyze)
- **Purpose Permissions**: Authorization tied to specific processing purposes (service delivery, analytics, marketing)
- **Disclosure Permissions**: Authorization for sharing with specific third parties or categories

> **Editor's Note**: The permissions_bundle bridges legal consent and technical enforcement. When an individual provides consent (legal basis), the permissions_bundle documents exactly what technical operations that consent authorizes. Without consent, permissions cannot be lawfully exercised for PII processing.

### 3.22 Shared Preferences (User-Controlled Settings)

Individual-controlled configuration settings that operate within the scope of granted consent and permissions. Shared preferences express how an individual chooses to exercise authorized permissions across services, contexts, or controllers.

**Shared Preferences Characteristics**:

- **Scope-Limited**: Can only configure options within already-granted permissions
- **Cross-Controller**: May be portable across controllers (e.g., "always decline marketing," "prefer minimal data collection")
- **Revocable**: Can be changed without requiring new consent if within existing permission scope
- **Non-Binding for New Processing**: Cannot authorize new processing that exceeds existing permissions

**Examples**:

- Privacy preference: "Minimize data collection where optional" (applies within existing consent)
- Communication preference: "Email preferred over SMS" (applies to already-authorized contact methods)
- Disclosure preference:  "Share with research partners" (only if secondary purpose consent includes research)

> **Editor's Note**: The distinction between consent, permissions, and shared preferences is critical for the co-regulatory model:

> - **Consent** = Legal basis (requires legal notice, free choice, withdrawal right controlled by individual)

> - **Permissions** = Technical implementation and enforcement of consent (what systems are authorized to do)

> - **Shared Preferences** = PII principal choices within permission scope (how individuals exercise their control)

> Traditional data protection conflates these concepts, treating online preference checkboxes as "consent." This profile separates them: consent is the legal basis used to grant permissions; permissions enable processing; shared preferences configure how that processing operates within authorized scope providing for  direct permissioning and autonomous consent withdrawl

### 3.23 Digitally Specified Consent

Consent as defined in Convention 108+ Article 5.2 ("freely given, specific, informed and unambiguous") operationalized through digital infrastructure that enables:

- **Controller identification before collection**: Controller-ID first architecture (Section 5.3)
- **Granular specification**: Through `permissions_bundle` fields documenting exact authorizations
- **Bilateral proof**: Via synchronized notice receipts held by both parties (Section 5.5)
- **Autonomous withdrawal**: Through Notice Event Log updates without controller gatekeeping (Section 7.1 #9)
- **Verifiable state**: Cryptographic signatures and public registry verification (Section 5.4.1)

**Critical Clarification**: This is **NOT a new legal basis for processing**—it is the technical operationalization of existing Convention 108+ Article 5.2 "specific, informed" consent requirements using verifiable digital infrastructure.

**Distinction from Traditional Consent Mechanisms**:

- **Traditional**: Privacy policy → tick box → unilateral controller record → manual withdrawal
- **Digitally Specified**: Public CIR → granular permissions review → bilateral receipt → autonomous withdrawal via Notice Event Log

**Legal Foundation**:

- Convention 108+ Article 5.2: Consent must be "freely given, specific, informed and unambiguous"
- GDPR Article 4(11): Same definition (jurisdictional implementation example)
- PIPEDA Schedule 1, Principle 4.3: "meaningful consent"
- Quebec Law 25 Article 14: "free and enlightened consent"

**What "Digitally Specified" Adds**:

- **Specification at scale**: Granular `permissions_bundle` enables specification impossible with analog consent forms
- **Verification at scale**: Bilateral receipts enable cryptographic proof of consent state
- **Withdrawal at scale**: Notice Event Log updates enable real-time consent revocation proportionate to real-time processing
- **Transparency at scale**: Public CIR registries enable regulatory oversight without manual audits

> **Editor's Note**: The term "digital consent" appears in earlier MVCR work and this profile's historical context. This profile operationalizes that vision as "digitally specified consent"—emphasizing that digital infrastructure enables **better implementation** of existing legal consent requirements, not creation of new legal basis. Courts, regulators, and privacy commissioners can assess this mechanism against existing consent validity criteria (freely given, specific, informed, unambiguous) without needing new legal frameworks.

---

### 3.23 Cross-Border Data Transfer

Transfer of personal data from one jurisdiction to another jurisdiction with different data protection legal authority and potentially different legal frameworks governing access, use, and protection of personal data.

### 3.24 Transfer Mechanism

Lawful basis enabling cross-border data transfer per Convention 108+ Article 14, establishing adequate safeguards through legal, contractual, or technical means to ensure continued data protection across jurisdictional boundaries.

### 3.25 Surveillance Risk

Risk that destination jurisdiction laws permit government access to transferred personal data without individual notification or consent, including foreign intelligence surveillance, national security data access, or lawful intercept programs.

> **Editor's Note**: Surveillance risk disclosure is material information required for informed consent in cross-border contexts. Examples include FISA Section 702 (USA), Investigatory Powers Act 2016 (UK), and national security access frameworks across jurisdictions. Transparency about destination jurisdiction legal regimes enables individuals to make informed decisions about cross-border data sharing.

Recognition by data protection authority that destination jurisdiction provides adequate safeguards per applicable framework, enabling cross-border transfers without additional contractual safeguards.

> **Editorial Note for v1.1**: Detailed adequacy determination protocols, mutual recognition frameworks, and registry verification mechanisms will be addressed in future revision. Current version enables controllers to disclose adequacy status through `transfer_mechanism="adequacy"` and `adequacy_status` field in `recipient_jurisdictions` object (Section 6.1.1.2) without requiring jurisdictional adequacy mapping.

### 3.27 Recipient Jurisdiction

Jurisdiction to which personal data is transferred for processing, storage, or disclosure, including legal authority governing data protection in that destination territory.

### 3.28 Consent Permission

Authorization state that combines legal consent (lawful basis under Convention 108+) with technical permissions (operational access controls in `permissions_bundle`). When `scope_of_disclosure` escalates to include processing not disclosed in the original consent, new consent permission is required through ANCR Exchange Stage 2 authorization, even if original consent remains valid for the original scope.

> **Editor's Note**: This term addresses the confusion between "consent" (legal basis) and "permissions" (technical controls) in scope escalation contexts. When a controller changes `scope_of_disclosure` from "regional" to "international", the original consent legal basis does not automatically authorize the expanded scope—new consent permission must be obtained that grants both legal authority AND updated technical permissions for the international transfer.

## Section 4: Abbreviated Terms

- **ANCR**: Anchored Notice and Consent Receipt
- **CIR**: Controller Identification Record
- **CIR-ID**: Controller Identification Record Identifier
- **MVCR**: Minimum Viable Consent Receipt (original Kantara Initiative specification)
- **2FN**: Two-Factor Notice
- **PII**: Personally Identifiable Information
- **WD**: Working Draft

> **Editorial Note for v1.1**: Advanced transparency features deferred to future revision include privacy preference signals (Section 4.4), transparency assurance indicators (Section 4.5), and Global Privacy Rights Controls framework (Section 4.6). These enhancements will be standardized in v1.1 after base co-regulated transparency infrastructure demonstrates adoption. See Appendix K for v1.1 preparation materials.

## Section 5: Universal Notice Receipt Architecture

### 5.1 Relationship to ISO/IEC 27560:2025

- Completes original MVCR to replace terms and conditions by default, that formed basis of ISO/IEC TS 27560:2023
- Extends 2025 WD (PII processing records for all lawful bases) with notice-first architecture
- Applies notice and consent receipt infrastructure to all six Convention 108+ legal bases
- Field-level compatible with PII processing record structure (Section 6.5)
- Uses base standard extensibility provisions
- Maintains backward compatibility with ISO/IEC TS 27560:2023 (see Appendix G)

### 5.2 Co-Regulated Transparency Infrastructure

**Key Innovation**: Notice and consent receipts can be generated **independently of controller** using publicly required information: (for example ICO Data Controller Registry)

1. Controller publishes CIR at /.well-known/transparency (or equivalent public location) recommend /notice.txt
2. CIR contains all fields required for notice receipt generation (party identification fields per ISO/IEC 27560:2025 Section 6.3.6)
3. Individual (or third-party service on individual's behalf) retrieves CIR
4. Notice receipt generated using CIR + context (notice type, timestamp, legal basis)
5. Both parties hold synchronized notice receipt without requiring controller-initiated generation

**Benefits**:

- Transparency-by-default: controller accountability precedes processing
- Surveillance resistance: individual can verify controller identity before providing any information
- Regulatory scalability: enforcement at scale through public CIR based transparency registries
- Legal basis flexibility: same infrastructure supports consent, contract, legal obligation, legitimate interest, vital interest, public interest

### 5.3 Anonymous-by-Default Architecture

- Removes pii_principal_id requirement from ANCR Exchange Stage 1 (Notice Receipt)
- Controller presents CIR before collecting individual identity
- Individual remains anonymous until choosing to authorize (ANCR Exchange Stage 2)
- Enables progressive identification: individual provides identifiers only when needed
- Preserves privacy across all lawful bases and contexts

### 5.4 Controller Identification Record (CIR)

- Structured from base standard party fields (Section 6.3.6)
- Scoped to Controller role (party_role="Controller")
- Contains: CIR-ID, legal name, jurisdiction, contact information, rights access point
- **Publicly accessible** (/.notice.txt/for-well-known/transparency or equivalent)
- Portable, verifiable, presented BEFORE any processing or interaction
- Enables registry verification and cross-jurisdictional lookup

**CIR Registrar Verification Infrastructure**:

- Controllers publish CIR as public accountability record
- Regulators maintain CIR registries for verification (e.g., ICO Controller Registry)
- **Registrars provide blind data notary function by default**: sign CIR upon registration without accessing PII Principal identifiers
- Individuals generate receipts using CIR + registrar signature—independently verified without controller cooperation
- Self-generated receipts validated against registrar's public key (published in registry)
- Third-party services can aggregate CIRs and validate receipts using registrar signatures

#### 5.4.1 Blind Data Notary Architecture

Controller registrars provide blind data notary signatures as digital public infrastructure:

**Blind Data Notary Properties**:

- Registrar signs CIR upon registration (controller identification record only)
- Signature does NOT access or require PII Principal identifiers
- Individual generates receipt locally using: CIR + context + registrar signature
- Receipt validation uses registrar's public key—no PII exposure to registrar or controller
- Notary may validate notice text independently from controller or principal to blindly notarise according to assurance requirements

**Privacy Through Architecture**:

- **What registrar signs**: CIR-ID, controller legal entity, jurisdiction, rights access point, publication timestamp
- **What registrar never sees**: pii_principal_id, individual identifiers, receipt content beyond CIR
- **Verification independence**: Third parties validate receipts against public registry without controller cooperation

**Contrast with Traditional Notarization**:

- Traditional: Notary witnesses transaction, accesses full content

- Blind data notary: Registrar signs controller identity record; individual generates receipt independently, delegates in person notarisation to authorised privacy officer

This architecture achieves high-assurance transparency (cryptographic proof) while  unlinked therefore preserving anonymous-by-default principle (registrar blind to PII Principal).

> **Editorial Note for v1.1**: CIR registrars provide blind data notary signatures by default, enabling Level 2 independent receipt verification. V1.1 will standardize:

> - **Level 1 (Self-Assertion)**: Controller unregistered, self-asserted CIR; notice receipts optional; suitable for minimal risk (local/child scope of disclosure)

> - **Level 2 (Registry Verification + Blind Data Notary)**: CIR-ID registered with authoritative source; registrar signature enables independent receipt validation; suitable for regional/community/national scope of disclosure

> - **Level 3 (Enhanced Transparency and Trust Officer Notarization)**: Transparency and Trust Officer certification with physical identity verification beyond registrar baseline; suitable for high-risk contexts requiring face-to-face liveliness assurance

> - **Level 4 (Active State + Physical Verification)**: Real-time validation mechanisms with remote attestation for critical infrastructure, high-risk AI, and vital interest contexts

> V1.1 will specify: Transparency and Trust roles  for privacy officer certification protocols for Level 3/4 enhanced assurance, cross-jurisdictional Transparency and Trust registry coordination, and active state remote validation mechanisms. Current version establishes registrar-native blind data notary as digital public infrastructure (Level 2); v1.1 addresses risk-proportionate Transparency and Trust Officer assurance gating for contexts requiring enhanced verification beyond registrar signatures.

### 5.4.1 notice.txt Structure

The CIR is published as a **notice.txt** file at /.well-known/transparency (or equivalent public location). This file uses a **risk-proportionate, additive structure** determined by:

1. **Scope of Disclosure** (geographic/categorical reach)
2. **PII Categories** (sensitive data types)
3. **Processing Context** (vulnerability factors)

#### Risk-Proportionate Field Requirements

#### Baseline (Zero/Minimal Risk)

Local-only processing, no disclosure, non-sensitive data only, controller id record is not required

```
notice_text: "We process personal data for service delivery."
lawful_basis: "consent"
processing_purposes: ["service_delivery"]
pii_categories: ["contact"]
```

```
rights_access_point: "privacy@example.local"
scope_of_disclosure: "local"
```

#### Low Risk (Child/Youth Scope)

Localized disclosure within community. Add controller identification:

```
controller_identity_record_id: "CIR-CA-12345"
controller_name: "Example Local Service"
jurisdiction: "CA-ON"
scope_of_disclosure: "child"
```

#### Medium Risk (Community/Regional Scope)

Regional processing or sensitive categories. Add processing details:

```
processing_locations: ["CA"]
retention_period: "12 months"
third_party_disclosure: false
data_protection_officer: "dpo@example.ca"
```

#### High Risk (National/International Scope)

Cross-border transfers, surveillance technologies, vulnerable populations. Add registry metadata and enhanced controls:

```
cir_publication_url: "https://registry.example.ca/CIR-CA-12345"
cir_registry: "ICO Data Controller Registry"
surveillance_risk_disclosure: true
```

#### Enhanced for Sensitive Categories

Additional requirements triggered by PII categories regardless of scope:

- **Special category data** (health, biometric, genetic): Add legal basis justification, explicit consent mechanism
- **Children's data**: Add parental verification, age-appropriate language
- **Financial data**: Add security certifications, breach notification timeline
- **Location data**: Add real-time tracking notice, geofencing disclosure

**Scope of Disclosure Categories** (from Section 3.6):

- **Local**: Device-only, no network disclosure (minimal risk)
- **Child/Youth**: Limited community disclosure (low risk)
- **Vulnerable**: Specific vulnerability context (context-dependent risk)
- **Community**: Local network disclosure (medium risk)
- **Regional**: Within jurisdiction boundaries (medium-high risk)

- **National**: Cross-regional within country (high risk)
- **International**: Cross-border disclosure (highest risk)

**Key Principles**:

- **Risk-proportionate**: Fields required based on actual disclosure risk and data sensitivity
- **Additive structure**: Higher risk requires baseline fields plus additional transparency
- **Scope-driven**: Geographic reach determines transparency granularity
- **Category-sensitive**: Sensitive PII categories trigger additional requirements regardless of scope
- **Machine-readable**: JSON or similar structured format for automated verification

### 5.5 Two-Factor Notice (2FN) Pattern

- Controller presents notice AND generates notice receipt
- Both parties hold synchronized receipt at issuance
- Provides proof-of-notice for both controller and individual
- Non-repudiation: controller cannot claim individual was not notified
- Applicable to safety, security, environment, privacy notifications

### 5.6 Notice Event Log

- Append-only audit trail of notice receipt lifecycle
- Logs: receipt issuance, authorizations granted, material changes, rights exercises
- Maintained by controller, queryable by individual via CIR rights access point
- Supports regulatory compliance and dispute resolution
- Universal across all notice contexts

### 5.7 Universal Notice Receipt Pattern

**ANCR Exchange Stage 1 (MANDATORY): Notice Receipt (or privacy notice receipt)**

- Controller presents CIR (or individual retrieves from public location)
- Notice receipt generated with notice_type (notification, disclosure, policy, signal)
- No pii_principal_id required
- Authorization: Notice acknowledgment (bilateral proof)

**ANCR Exchange Stage 2 (CONDITIONAL): Consent Notice Receipt**

- Individual returns receipt with authorization
- authorization_type varies by context and legal basis
- Optional: pii_principal_id to link to account
- Enables secondary purpose consent using existing receipt

**ANCR Exchange Stage 3 (OPTIONAL): Micro Notice Credential**

- Cryptographic signature for technical contexts
- Enables API authorization, cross-device sync, remote verification

**ANCR Exchange Stage 4 (OPTIONAL): Consent Token**

- Individual-controlled token with principal anchor
- Enables agentic coordination, authorization wallet, directed authorization

## Section 6: ANCR Exchange Stage 1 Field Specification

### 6.1 Mapping to ISO/IEC 27560:2025 Section 6.5

ANCR Exchange Stage 1 (Notice Receipt) organizes fields into base standard structure:

**Record Header**:

- schema_version: "27560-UNIVERSAL-NOTICE-2025-1.0"
- receipt_id: Unique receipt identifier
- **pii_principal_id: REMOVED** (ANCR Exchange Stage 1 only; optional Stage 2+)
- controller_identity_record_id: CIR-ID for verification
- notice_receipt_type: "ANCR Exchange Stage 1"
- notice_type: "notification" | "disclosure" | "policy" | "signal"
- two_factor_notice_indicator: true

**Notice Context Section**:

- All base standard fields from Section 6.3.4 (adapted for universal contexts)
- context_category: "privacy" | "safety" | "security" | "environment"
- scope_of_disclosure: Risk category (child, youth, vulnerable, community, regional, national, international)
- permissions_bundle: Granular permissions proposed (ANCR Exchange Stage 1) or granted (ANCR Exchange Stage 2)

**Controller Identification (CIR)**:

- All base standard party fields from Section 6.3.6
- party_role: "Controller"
- party_id: CIR-ID
- cir_publication_url: Public location of CIR (e.g., /.well-known/transparency)
- rights_access_point: URL or contact for exercising rights
- notice_event_log_url: Endpoint for state queries

**Event Section**:

- event_time: Notice issuance timestamp
- event_type: "notice_issued"

- entity_id: CIR-ID

### A.1 Field-Level Mapping Overview

This appendix provides the complete field mapping between the Universal Notice Receipt Profile and ISO/IEC 27560:2025 base standard structure. All fields maintain compatibility with Section 6.5 of the base standard.

### A.2 Stage 1 Architectural Modifications

**Removed Fields in ANCR Exchange Stage 1**:

- **pii_principal_id**: Removed from Stage 1 to enable anonymous-by-default architecture (optional in Stage 2+)

**New Fields for Universal Notice Receipt Profile**:

- **controller_identity_record_id**: CIR-ID for public registry verification
- **cir_publication_url**: Public location of Controller Identification Record
- **notice_receipt_type**: Stage progression identifier (ANCR Exchange Stage 1-4)
- **notice_type**: Context categorization (notification, disclosure, policy, statement, signal)
- **context_category**: Domain categorization (privacy, safety, security, environment, ai_system)
- **two_factor_notice_indicator**: Boolean flag for 2FN pattern implementation
- **scope_of_disclosure**: Risk-proportionate transparency category
- **permissions_bundle**: Granular permission/authorization array
- **authorization_type**: Stage 2+ semantic variation by legal basis and context

### A.3 Base Standard Field Adaptations

**Record Header Section** (ISO/IEC 27560:2025 Section 6.3.3):

- `schema_version` → "27560-UNIVERSAL-NOTICE-2025-1.0"
- `record_id` → `receipt_id` (semantic clarity)
- `pii_principal_id` → Optional in Stage 1; Conditional in Stage 2+

**Context Section** (ISO/IEC 27560:2025 Section 6.3.4):

- All base standard context fields adapted for universal contexts (privacy, safety, security, environment)
- `processing_purposes` → Applicable to all legal bases and contexts
- `pii_categories` → Extended to include safety/security/environment data categories
- `processing_locations` → Used for `scope_of_disclosure` risk determination
- `codes_of_conduct` → References Convention 108+ as normative framework

**Party Section** (ISO/IEC 27560:2025 Section 6.3.6):

- Controller party fields structured as CIR (Controller Identification Record)

- `party_role` → "Controller" (CIR scope)
- `party_id` → Enhanced as `controller_identity_record_id` with registry verification
- All controller contact fields publicly accessible via CIR

**Event Section** (ISO/IEC 27560:2025 Section 6.3.7):

- `event_time` → Notice issuance timestamp
- `event_type` → Extended for universal contexts: notice_issued, consent_granted, safety_acknowledged, security_policy_accepted, environmental_disclosure_acknowledged
- Notice Event Log captures all state changes across contexts

### A.4 Cross-Border Transfer Field Additions

When `scope_of_disclosure="national"` or `"international"`:

- **transfer_mechanism**: Lawful basis for cross-border transfer (consent, contract, adequacy, scc, bcr, legitimate_interest, derogation)
- **recipient_jurisdictions**: Array of ISO 3166-1 alpha-2 country codes (or objects with enhanced disclosure)
- **surveillance_risks**: Object documenting government access risks in destination jurisdictions
- **transfer_consent_validation**: Object proving informed consent for cross-border transfers
- **pii_principal_jurisdiction**: Optional field identifying individual's legal jurisdiction

### A.5 Authorization Exchange Field Progression

**ANCR Exchange Stage 2 Additions**:

- `authorization_type`: Semantic variation by legal basis (consent_granted, contract_accepted, legal_obligation_acknowledged, etc.)
- `consent_timestamp`: When authorization granted
- `pii_principal_id`: Optional identifier linking to account

**ANCR Exchange Stage 3 Additions**:

- `cryptographic_signature`: Signature over receipt + permissions
- `credential_binding`: Device ID, session ID, API key
- `technical_permissions_scope`: API endpoints, data operations
- `validity_period`: Credential expiration

**ANCR Exchange Stage 4 Additions**:

- `principal_anchor`: DID, public key, wallet address
- `token_claims`: Issuer, subject, audience, expiration
- `cross_controller_metadata`: Original CIR-ID, provenance chain
- `portability_scope`: Geographic, jurisdictional, purpose restrictions

### A.6 Backward Compatibility with ISO/IEC TS 27560:2023

See Appendix G for complete migration guidance from 2023 TS to Universal Notice Receipt Profile.

**Key Compatibility Notes**:

- Universal notice receipts can be exchanged with 2023 TS systems
- `schema_version` field enables version detection
- 2023 systems interpret universal notice receipts as consent receipts (ignore new fields)
- Universal systems read 2023 receipts and map to ANCR Exchange Stage 2 consent context

> **Editorial Note**: Detailed field-by-field mapping tables with cardinality, data types, and ISO/IEC 27560:2025 clause references will be provided in the final submission version. Current version establishes architectural modifications and new field requirements for universal context applicability.

### 6.2 Key Modifications from Base Standard

### 6.1.1 codes_of_conduct Field

ISO/IEC 27560:2025 WD includes `codes_of_conduct` field (clause 6.3.4.20) enabling controllers to reference sector-specific or jurisdictional codes of conduct.

**Data type**: String or Object

**Cardinality**: Optional

**Description**: This profile uses `codes_of_conduct` to reference Convention 108+ as the normative legal framework, with the profile serving as technical implementation specification.

**Structured Format** (Recommended):

```
{
  "codes_of_conduct": {
    "legal_framework": "Council of Europe Convention 108+",
    "implementation_profile": "ISO/IEC 27560 Universal Notice Receipt Profile v1.0",
    "conformance_level": "Universal Notice Receipt",
    "tata_level": 2,
    "jurisdiction": "CA",
    "supervisory_authority": "https://www.priv.gc.ca"
  }
}
```

**Simple String Format** (Backward Compatible):

```
{
  "codes_of_conduct": "Council of Europe Convention 108+ operationalized via ISO/IEC 27
560 Universal Notice Receipt Profile v1.0"
}
```

**Field Values**:

- **legal_framework**: Treaty or legislative framework (e.g., "Council of Europe Convention 108+", "GDPR", "PIPEDA")
- **implementation_profile**: Technical standard implementing the framework (e.g., "ISO/IEC 27560 Universal Notice Receipt Profile v1.0")
- **conformance_level**: "Universal Notice Receipt" | "Authorization Exchange" | "Full Protocol"
- **tata_level**: 1 (Self-Assertion), 2 (Registry Verification), 3 (Notarized Receipts), 4 (Physical Verification + Active State)
- **jurisdiction**: ISO 3166-1 alpha-2 or alpha-3 country code
- **supervisory_authority**: URL of competent supervisory authority under Convention 108+ or applicable framework

**Rationale**:

- Positions Convention 108+ as authoritative framework rather than creating new code of conduct
- Enables jurisdictional customization while maintaining treaty baseline
- Provides machine-readable reference for automated verification
- Links controller to supervisory authority for enforcement coordination

**Usage Example**:

```
{
  "controller_identity_record_id": "CIR-CA-12345",
  "codes_of_conduct": {
    "legal_framework": "Council of Europe Convention 108+",
    "implementation_profile": "ISO/IEC 27560 Universal Notice Receipt Profile v1.0",
    "conformance_level": "Authorization Exchange",
    "tata_level": 2,
    "jurisdiction": "CA",
    "supervisory_authority": "https://www.priv.gc.ca"
  },
  "cir_publication_url": "https://example.ca/.well-known/transparency"
}
```

### 6.1.2 Cross-Border Transfer Fields

When `scope_of_disclosure` includes "national" or "international", the following fields provide transparency for cross-border data transfers per Convention 108+ Article 14:

#### 6.1.2.1 transfer_mechanism

Lawful mechanism enabling cross-border data transfer.

**Data type**: String (enum)

**Cardinality**: Conditional (mandatory when scope_of_disclosure="national" or "international")

**Values**:

- "consent": Explicit consent for cross-border transfer
- "contract": Transfer necessary for contract performance
- "adequacy": Adequacy decision by competent authority
- "scc": Standard Contractual Clauses
- "bcr": Binding Corporate Rules
- "legitimate_interest": Legitimate interest with balancing test
- "derogation": Specific derogation under applicable law

**Rationale**: Convention 108+ Article 14 requires adequate safeguards for transborder flows of personal data. This field documents the legal mechanism enabling compliant cross-border transfers.

**Example**:

```
{
  "scope_of_disclosure": "international",
  "transfer_mechanism": "consent",
  "processing_locations": ["CA", "US"]
}
```

#### 6.1.2.2 recipient_jurisdictions

ISO 3166-1 alpha-2 country codes for data transfer destination jurisdictions.

**Data type**: Array of strings (ISO 3166-1 alpha-2 codes) OR array of objects for enhanced transparency

**Cardinality**: Conditional (mandatory when scope_of_disclosure="national" or "international")

**Basic Format**:

```
{
  "recipient_jurisdictions": ["US", "GB", "AU"]
}
```

**Enhanced Format** (recommended for high-risk transfers):

```
{
  "recipient_jurisdictions": [
    {
      "country_code": "US",
      "adequacy_status": "no_decision",
      "legal_regime": "FISA Section 702 permits government access to data of non-US persons",
      "transfer_safeguards": ["Standard Contractual Clauses", "Supplementary measures per Schrems II"]
    },
    {
      "country_code": "CA",
      "adequacy_status": "adequate",
      "legal_regime": "PIPEDA substantial similarity with Convention 108+",
      "transfer_safeguards": []
    }
  ]
}
```

**Object Structure** (when using enhanced format):

- **country_code** (string, required): ISO 3166-1 alpha-2 code
- **adequacy_status** (string enum, optional): "adequate" | "no_decision" | "restricted"
- **legal_regime** (string, optional): Description of destination jurisdiction data protection framework
- **transfer_safeguards** (array of strings, optional): Technical or organizational safeguards applied

**Rationale**: Enables individuals to verify data destinations and assess jurisdiction-specific risks. Enhanced format provides material information for informed consent in cross-border contexts.

---

#### 6.1.2.3 surveillance_risks

Disclosed surveillance or government access risks associated with cross-border transfers to enable informed consent.

**Data type**: Object

**Cardinality**: Conditional (mandatory when transfer_mechanism="consent" AND recipient lacks adequacy decision)

> **Editorial Note for v1.1**: Current version requires basic surveillance risk disclosure (disclosed boolean + summary description). Enhanced disclosure with jurisdiction-specific legal framework mapping (jurisdictions object with mitigation_measures and legal_frameworks arrays) is RECOMMENDED but not mandatory for v1.0. V1.1 will standardize surveillance risk registry with vetted legal framework descriptions per jurisdiction, enabling automated risk disclosure updates as laws change.

**Object Structure**:

- **disclosed** (boolean, required): Whether surveillance risks have been disclosed to individual

- **jurisdictions** (object, optional): Map of country code to risk description
- **mitigation_measures** (array of strings, optional): Technical/organizational safeguards implemented
- **legal_frameworks** (array of strings, optional): Specific laws or frameworks enabling government access

**Example (Cross-border transfer with foreign intelligence surveillance disclosure)**:

```
{
  "transfer_mechanism": "consent",
  "recipient_jurisdictions": ["US"],
  "surveillance_risks": {
    "disclosed": true,
    "jurisdictions": {
      "US": "The United States Foreign Intelligence Surveillance Act (FISA) Section 702 permits government access to data of non-US persons without individual notification. Data transferred to US cloud providers may be subject to lawful government access requests."
    },
    "mitigation_measures": [
      "End-to-end encryption for data at rest",
      "Data minimization—only essential fields transferred",
      "Regular transparency reports on government requests"
    ],
    "legal_frameworks": [
      "Foreign Intelligence Surveillance Legislation",
      "CLOUD Act (18 U.S.C. § 2713)"
    ]
  }
}
```

```
{
  "transfer_mechanism": "consent",
  "recipient_jurisdictions": ["US"],
  "surveillance_risks": {
    "disclosed": true,
    "jurisdictions": {
      "US": "Foreign intelligence surveillance legislation permits government access to data of non-US persons without individual notification. Data transferred to US cloud providers may be subject to lawful government access requests."
    },
    "mitigation_measures": [
      "End-to-end encryption for data at rest",
      "Data minimization—only essential fields transferred",
      "Regular transparency reports on government requests"
    ],
    "legal_frameworks": [
      "FISA Section 702 (50 U.S.C. § 1881a)",
      "CLOUD Act (18 U.S.C. § 2713)"
    ]
  }
}
```

**Example (Multiple destination jurisdictions)**:

```
{
  "surveillance_risks": {
    "disclosed": true,
    "jurisdictions": {
      "US": "Foreign intelligence surveillance legislation permits government access to data of non-US persons without notification",
      "GB": "Investigatory Powers Act 2016 permits bulk data access by intelligence agencies",
      "AU": "Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 permits compelled technical assistance"
    },
    "mitigation_measures": [
      "Data segregation by jurisdiction",
      "Individual notification upon lawful government request (where legally permitted)"
    ],
    "legal_frameworks": [
      "FISA Section 702 (USA)",
      "Investigatory Powers Act 2016 (UK)",
      "TOLA Act 2018 (Australia)"
    ]
  }
}
```

**Rationale**: Informed consent for cross-border transfers under Convention 108+ Article 14 (as implemented in EU Regulation 2018/1725 Article 68) requires disclosure of material risks, including government surveillance or access under destination jurisdiction laws. Transparency about legal frameworks like foreign intelligence surveillance legislation enables individuals to make informed decisions about cross-border data sharing.

**Legal Basis**:

- Convention 108+ Article 14: Adequate safeguards required for transborder flows
- EU Regulation 2018/1725 Article 68: Transfers of personal data to third countries or international organisations (operational implementation)
- CJEU *Schrems II* (C-311/18): Jurisdictional example invalidating Privacy Shield due to foreign intelligence surveillance risks

- EDPB Recommendations 01/2020: Jurisdictional guidance on supplementary measures

### 6.1.2.4 transfer_consent_validation

Fields documenting that consent for cross-border transfer was informed, specific, and valid at the time of transfer authorization.

**Data type**: Object

**Cardinality**: Conditional (mandatory when transfer_mechanism="consent")

**Object Structure**:

- **transfer_consent_timestamp** (ISO 8601 datetime, required): When consent for cross-border transfer was granted
- **surveillance_disclosed_at_consent** (boolean, required): Whether surveillance risks were disclosed before consent
- **transfer_purpose** (string, required): Specific purpose for cross-border transfer
- **withdrawal_mechanism** (string, required): How individual can withdraw cross-border transfer consent
- **consent_evidence_id** (string, optional): Reference to Notice Event Log entry proving consent

**Example**:

```
{
  "transfer_mechanism": "consent",
  "transfer_consent_validation": {
    "transfer_consent_timestamp": "2025-12-11T10:30:00-05:00",
    "surveillance_disclosed_at_consent": true,
    "transfer_purpose": "Cloud storage for service delivery—data processed in US data centers",
    "withdrawal_mechanism": "Email privacy@example.com to withdraw cross-border transfer consent"
  }
}
```

**Rationale**: Demonstrates compliance with informed consent requirements for cross-border transfers. Proves that individual was aware of surveillance risks at the time consent was granted, addressing *Schrems II* transparency requirements.

### 6.1.2.5 pii_principal_jurisdiction

Legal jurisdiction where the PII Principal resides or is located at time of processing, enabling risk-appropriate cross-border transfer disclosure.

**Data type**: String (ISO 3166-1 alpha-2 or ISO 3166-2 for subdivisions)

**Cardinality**: Optional in ANCR Exchange Stage 1; Conditional in Stage 2+ (recommended when scope_of_disclosure="national" or "international")

> **Editorial Note for v1.1**: This field is OPTIONAL in v1.0 to maintain anonymous-by-default architecture simplicity. V1.1 will standardize risk-proportionate jurisdiction determination protocols including: determination method disclosure requirements, accuracy guarantee standards, correction mechanisms for inaccurate inferences, and privacy-preserving alternatives (e.g., jurisdiction range rather than precise location). V1.0 enables cross-border transparency using controller_jurisdiction and recipient_jurisdictions without requiring individual location inference.

**Determination Methods** (should be disclosed via `jurisdiction_determination_method` field):

- **self_declared**: Individual explicitly provided jurisdiction
- **ip_geolocation**: Inferred from IP address (disclose accuracy limitations)
- **account_registration**: Derived from account profile or billing address
- **payment_method**: Inferred from payment billing jurisdiction
- **locale_inference**: Derived from browser/device locale settings

**Basic Format**:

```
{
  "pii_principal_jurisdiction": "CA",
  "jurisdiction_determination_method": "self_declared"
}
```

**Enhanced Format** (recommended for cross-border consent):

```
{
  "pii_principal_jurisdiction": "CA-ON",
  "jurisdiction_determination_method": "account_registration",
  "determination_timestamp": "2025-12-12T06:30:00-05:00",
  "determination_accuracy": "high"
}
```

**Use Cases**:

**1. Cross-Border Transfer Risk Assessment**:

Enables controller to determine if transfer from PII Principal's jurisdiction to recipient jurisdiction requires enhanced disclosure.

```
{
  "pii_principal_jurisdiction": "CA",
  "controller_jurisdiction": "CA",
  "recipient_jurisdictions": ["US"],
  "transfer_mechanism": "consent",
  "surveillance_risks": {
    "disclosed": true,
    "jurisdictions": {
      "US": "As a Canadian resident, FISA Section 702 permits US government access to your data without notification when transferred to US providers."
    }
  }
}
```

**2. Jurisdictional Rights Determination**:

Identifies which data protection framework applies to individual's rights.

```
{
  "pii_principal_jurisdiction": "EU-DE",
  "applicable_rights_framework": "GDPR",
  "rights_access_point": "dpo@example.eu"
}
```

**3. Surveillance Risk Materiality**:

Determines which surveillance laws affect the individual based on their jurisdiction.

- Non-US persons: FISA Section 702 surveillance risks material
- US persons: Different surveillance framework applies
- EU residents: Schrems II adequacy considerations apply

**4. Adequacy Assessment**:

```
{
  "pii_principal_jurisdiction": "GB",
  "recipient_jurisdictions": ["US"],
  "adequacy_assessment": {
    "from_jurisdiction": "GB",
    "to_jurisdiction": "US",
    "adequacy_status": "no_decision",
    "safeguards_required": ["Standard Contractual Clauses", "Supplementary measures"]
  }
}
```

**Privacy Considerations**:

- **ANCR Exchange Stage 1**: Do NOT collect—maintains anonymous-by-default
- **ANCR Exchange Stage 2+**: Collect only when necessary for cross-border transfer disclosure
- **Granularity**: Use country-level (CA) unless subdivision is material (CA-ON for provincial law differences)
- **Inference disclosure**: If using IP geolocation or inference, disclose method and accuracy

- **Update mechanism**: Allow individual to correct if determination is inaccurate or jurisdiction changes

**Rationale**:

- Enables **risk-proportionate transparency** for cross-border transfers based on PII Principal's actual jurisdiction
- Supports **informed consent** by tailoring surveillance risk disclosure to individual's legal context
- Facilitates **jurisdictional rights exercise** by identifying applicable data protection framework
- Addresses **Schrems II requirements** for assessing adequacy based on data subject's jurisdiction
- Enables **material risk disclosure**: surveillance laws affect individuals differently based on their nationality/residence

**Legal Basis**:

- Convention 108+ Article 14: Cross-border transfer safeguards depend on both source and destination jurisdiction
- EU Regulation 2018/1725 Article 68: Transfer risk assessment considers data subject's jurisdiction
- CJEU *Schrems II* (C-311/18): Adequacy determination depends on protection level in data subject's jurisdiction
- GDPR Article 44: Cross-border transfer restrictions protect EU/EEA residents specifically

---

**Integration with Existing Fields**:

Cross-border transfer fields integrate with existing profile architecture:

- **scope_of_disclosure**: Triggers cross-border field requirements when set to "national" or "international"
- **processing_locations**: Works with recipient_jurisdictions to document full data flow
- **permissions_bundle**: Cross-border transfer requires explicit "disclose_international" permission
- **Notice Event Log**: Records transfer_consent_timestamp and material changes to surveillance_risks
- **authorization_type**: "consent_granted" with cross-border context requires all validation fields

**Conformance Requirement** (addition to Section 7.1):

1. **Cross-Border Transparency**: When scope_of_disclosure="national" or "international", SHALL:
    - Specify transfer_mechanism for all cross-border transfers

- Disclose surveillance_risks when transfer_mechanism="consent" and destination lacks adequacy decision
- Provide transfer_consent_validation fields demonstrating informed consent
- Document recipient_jurisdictions with ISO 3166-1 alpha-2 codes

### 6.2 Key Modifications from Base Standard

**Removed**: pii_principal_id (ANCR Exchange Stage 1 only)

**Rationale**: Base standard assumes controller creates record AFTER obtaining permission. Universal notice receipt inverts this: controller publishes CIR, notice receipt generated BEFORE processing/interaction begins.

**New Fields**:

- controller_identity_record_id: CIR-ID for registry verification
- cir_publication_url: Public location of CIR
- notice_receipt_type: Stage progression tracker
- notice_type: Context categorization (notification, disclosure, policy)
- context_category: Domain categorization (privacy, safety, security, environment)
- two_factor_notice_indicator: 2FN pattern flag
- scope_of_disclosure: Risk-proportionate transparency
- permissions_bundle: Granular permission/authorization management

### 6.3 Addressing Data Protection Limitations

This profile addresses critical gaps in traditional data protection approaches:

**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 only proportionate when (provided in person)

**3. Consent**: All six Convention 108+ legal bases vs. consent-only scope

**4. Authorization**: ANCR Exchange Stage 4 (Consent Token) vs. no cross-controller portability

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

**6. Transparency Standard**: Convention 108+ as standard public privacy policy by default (notice.txt at /.well-known/transparency) vs. custom privacy policies per controller (lengthy, incompatible, unverifiable)

**7. Proof**: Bilateral receipts (2FN, both parties hold synchronized proof) vs. unilateral controller records

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

**9. Revocation**: Immediate via Notice Event Log update vs. requires controller cooperation

**10. Enforcement**: Automated receipt verification via public registries (scales) vs. manual audits (cannot scale)

**Key Innovation**: By implementing Convention 108+ horizontal transparency requirements as digital public infrastructure through notice.txt, this profile establishes a **universal baseline privacy policy standard** that enables comparison, verification, and enforcement at scale—addressing the fundamental data protection gap where each organization creates incompatible, unverifiable transparency mechanisms.

---

## Section 7: Universal Notice Receipt Conformance

### 7.1 Mandatory for Universal Notice Receipt Profile Conformance

1. **CIR Publication**: SHALL publish Controller Identification Record at publicly accessible location BEFORE any processing or interaction
2. **CIR Public Accessibility**: SHALL make CIR accessible without authentication (anonymous access)
3. **Anonymous-by-Default**: ANCR Exchange Stage 1 (Notice Receipt) SHALL NOT require pii_principal_id or any individual identifier
4. **Two-Factor Notice**: SHALL implement 2FN for all contexts requiring bilateral proof
5. **Notice Event Log**: SHALL maintain append-only log accessible to individuals via CIR rights access point
6. **Scope of Disclosure**: SHALL specify risk category for all processing/interaction activities
7. **Field Compatibility**: SHALL use base ISO/IEC 27560:2025 field definitions (with universal context extensions)
8. **Context Applicability**: SHALL support notice receipts across privacy, safety, security, environment contexts
9. **Scope Escalation Consent Permission**: When `scope_of_disclosure` changes to include "national" or "international" processing that was not disclosed in the original notice, controllers SHALL:
    - Issue material change notification (notice_type="disclosure")
    - Generate new ANCR Exchange Stage 1 (Notice Receipt) with updated `scope_of_disclosure`, `recipient_jurisdictions`, and `surveillance_risks` (if applicable)
    - Obtain new ANCR Exchange Stage 2 consent permission authorization before implementing the expanded scope
    - Record scope escalation and new consent permission timestamp in Notice Event Log
    - **EXCEPTION**: If individual presents valid ANCR Exchange Stage 4 (Consent Token) with `portability_scope` covering the new destination jurisdiction(s), new consent permission is not required

### 7.2 Optional Enhancements

- CIR registry participation (recommended for cross-jurisdictional verification)

- ANCR Exchange Stage 2-4 authorization exchange protocol extensions
- Cryptographic signatures for high-assurance contexts
- Principal-anchored tokens for authorization portability

## Section 8: Universal Context Applications

### 8.1 Privacy Context

Notice receipts for PII processing under any lawful basis:

- **Consent**: Secondary purpose consent using existing ANCR Exchange Stage 1 receipt
- **Contract**: Individual-proffered terms pattern
- **Legal Obligation**: Regulatory transparency enforcement
- **Legitimate Interest**: Balancing test transparency with opt-out
- **Vital Interest**: Emergency authority coordination
- **Public Interest**: Research, journalism, archiving transparency

### 8.2 Safety Context

Notice receipts for safety-critical notifications:

- **Product Recalls**: Manufacturer presents CIR + recall details, bilateral receipt proves notification
- **Hazard Warnings**: Equipment operators receive notice receipt for hazardous condition acknowledgment
- **Emergency Notifications**: Public safety authorities issue notice receipts for evacuation orders, emergency alerts

#### 8.2.1 Risk-Based Authentication for Safety Contexts

Authentication according to risk provides for new forms of authentication that are fit for purpose and context. Safety contexts demonstrate proportionality principles across the four TATA levels:

**Level 1 (Device/Local - Minimal Risk):**

Consumer product with local-only processing (e.g., standalone smoke detector). CIR presentation sufficient without authentication—controller identification before individual identification enables anonymous safety notification access.

**Level 2 (Community/Regional - Proportionate Risk):**

Product recall notification within jurisdiction. Controller registry verification + notice receipt acknowledgment. Authentication proportionate to disclosure scope—regional hazard requires verifiable controller, not necessarily verified individual.

**Level 3 (National/International - Enhanced Risk):**

Cross-border hazardous materials disclosure. Cryptographic signatures on notice receipts (ANCR Exchange Stage 3) enable remote verification. High-risk contexts require enhanced transparency—international scope triggers Convention 108+ Article 14 cross-border safeguards.[1][2]

**Level 4 (Critical Infrastructure - High Assurance):**

Emergency response coordination requiring real-time active state signaling. Face-to-face liveness assurance for break-the-glass scenarios. Vital interest legal basis permits emergency processing while maintaining bilateral proof of notification for post-facto accountability.

**Level 4 Dynamic Liability Transfer for Digital Privacy Risk Mitigation:**

At TATA Level 4, **Privacy Rights Controls dynamically transfer liability from Controller to PII Principal when specific conditions are met**, enabling individual-controlled risk management through informed consent:

**Conditions for Dynamic Liability Transfer:**

1. **Active State Transparency**: Real-time CIR hash validation (Section 17.2.1) proves current transparency state
2. **Explicit Informed Consent**: PII Principal acknowledges specific digital privacy risks disclosed via `surveillance_risks` and `rights_derogations` fields (Section 6.1.2.3)
3. **Bilateral Proof**: Notice Event Log records `derogation_disclosed_at_consent=true` with timestamp
4. **Individual Control Activation**: PII Principal exercises Privacy Rights Controls through consent token (ANCR Exchange Stage 4)

**How Liability Transfers:**

**Controller Liability (Before Transfer):**

- Controller responsible for transparency failures
- Controller liable for undisclosed surveillance risks
- Controller accountable for rights derogations without notice
- Regulatory enforcement targets controller for non-compliance

**PII Principal Liability (After Transfer):**

- **When conditions met**: Individual assumes responsibility for digital privacy risk **within disclosed scope**
- Individual **knowingly accepts** cross-border transfer to FISA 702 jurisdiction after explicit disclosure
- Individual **knowingly accepts** rights derogations (e.g., suspension of right to access under national security law) after explicit disclosure
- Individual controls withdrawal—removes acceptance dynamically by updating Notice Event Log

**Key Distinction**: Liability transfers for **disclosed risks only**—controller remains liable for:

- Undisclosed processing activities
- Scope escalation beyond consented disclosure

- Failure to maintain Notice Event Log accuracy
- Violation of bilateral receipt terms

**Example Scenario:**

**Scenario**: Cross-border transfer to US cloud provider subject to FISA Section 702

**Without Level 4 (Traditional Data Protection):**

- Controller says "adequate safeguards in place"
- Individual clicks "Accept"
- **If government accesses data**: Controller liable for inadequate safeguards (Schrems II outcome)

**With Level 4 (Dynamic Liability Transfer):**

1. Controller publishes CIR with `surveillance_risks` disclosure: "FISA Section 702 permits US government access to data of non-US persons without notification"
2. Controller publishes `rights_derogations`: "right_to_access", "right_to_be_informed_of_processing" suspended under national security derogation
3. PII Principal reviews disclosure via ANCR Exchange Stage 1 (Notice Receipt)
4. PII Principal **explicitly authorizes transfer** via ANCR Exchange Stage 2 with `authorization_type="consent_granted"` AND `surveillance_disclosed_at_consent=true`
5. **Liability transfers**: Individual has accepted disclosed surveillance risk
6. **If government accesses data**: Controller protected—individual was informed and consented to known risk
7. **If controller adds NEW undisclosed risk** (e.g., transfers to China without notice): Liability remains with controller—scope escalation violates bilateral receipt terms

**Dynamic Risk Mitigation Benefits:**

**For Controllers:**

- **Liability protection**: Proof of informed consent (bilateral receipt + Notice Event Log) demonstrates compliance
- **Regulatory defense**: Can prove to supervisory authorities that individual was informed of surveillance risks before consent
- **Schrems II compliance**: Explicit surveillance disclosure addresses CJEU transparency requirements

**For PII Principals:**

- **Informed control**: Can assess risk BEFORE providing data
- **Autonomous withdrawal**: Can revoke consent dynamically—liability transfers back to controller if withdrawal ignored
- **Portable consent**: Can carry consent token across controllers—risk acceptance is explicit, not assumed

**For Regulators:**

- **Scaled oversight**: Automated verification through CIR registries and Notice Event Logs
- **Adequacy determinations**: Can require `surveillance_disclosed_at_consent=true` for cross-border transfer approval
- **Enforcement evidence**: Bilateral receipts provide proof of informed consent or lack thereof

**Proportionality Principle Application:**

Level 4 liability transfer is **proportionate to digital privacy risk**:

- **Low risk** (local processing): No liability transfer needed—minimal risk to manage
- **High risk** (cross-border to surveillance jurisdiction): Liability transfer **appropriate**—individual can assess and accept known risk OR reject and choose alternative
- **Derogated rights contexts**: Liability transfer **necessary**—individual must know which rights are suspended to make informed decision

**Legal Foundation:**

Convention 108+ Article 5.2 (informed consent) + Article 11.3 (proportionate derogations) + Article 14 (cross-border safeguards) = **Liability can transfer when individual is fully informed of risks and explicitly consents**

CJEU Schrems II: Privacy Shield failed because **individuals were not informed of surveillance risks**—no informed consent = no liability transfer = controller remains liable

This profile enables liability transfer **only when transparency conditions are met**—restoring individual autonomy while protecting controllers who provide genuine transparency.

**Legal Basis Alignment:**

Quebec Law 25 and Meaningful Consent Law require transparency and control over digital identification technologies, establishing that authentication strength must match digital privacy risk [7].

**AuthC Protocol Implementation:**

Safety contexts implement AuthC (Authorization with Consent) exchange:

- **Authority of Consent (Auth C + P)**: Controller authority to issue safety notification binds to purpose (hazard mitigation, recall compliance)
- **Authentication & Authorization (Auth N & Z)**: Authentication only when necessary for individual-specific safety action (e.g., personalized medical device recall)

This approach operationalizes transparency before authentication—controller identifies safety risk and legal authority before requesting individual verification.[8][9]

> **Editorial Note**: Citations [8] and [9] reference Convention 108+ Articles 8(2) and 9 respectively. These citations will be added to Section 2.4 Legal References in the final submission version.

**Cross-Context Consistency:**

Same proportionality framework applies across privacy, security, and environment contexts. Scope of disclosure determines authentication requirements—not controller preferences or legacy systems. Risk-proportionate authentication enables:

- Emergency notifications without authentication barriers
- Post-facto accountability through bilateral receipts
- Regulatory enforcement through public CIR registries
- International safety coordination without identification proliferation

### 8.3 Security Context

Notice receipts for security policies and incidents:

- **Acceptable Use Policies**: Organizations issue notice receipts for security policy acknowledgment
- **Security Incident Disclosures**: Breach notifications with bilateral proof of notification
- **Access Control Policies**: Authorization rules documented via notice receipts

### 8.4 Environment Context

Notice receipts for environmental disclosures:

- Tracking environmental impact of online choices and alternatives
- **Environmental Impact Disclosures**: Companies issue notice receipts for sustainability reporting
- **Hazardous Waste Notifications**: Proximity disclosures with bilateral proof
- **Climate Risk Disclosures**: Financial institutions document climate risk notifications
- Supply chain authenticity

### 8.5 Cross-Context Benefits

Same base requirements enable:

- **Unified accountability infrastructure**: Single CIR serves all contexts
- **Regulatory efficiency**: One verification mechanism across domains
- **Individual empowerment**: Consistent rights access across contexts
- **Audit trail consistency**: Notice Event Log tracks all notification types
- This simplifies transparency over safety security and privacy for all stakeholders

## Section 9: Security and Privacy Considerations

### 9.1 Anonymous-by-Default Privacy

- Controller cannot identify individual unless individual chooses to link
- Notice-by-default through interaction with CIR
- Progressive identification: individual provides identifiers only when needed

- Universal across privacy, safety, security, environment contexts

**9.2 Two-Factor Notice Security**

- Proof-of-notice for both parties prevents non-repudiation
- Synchronized state enables accountability
- Cryptographic proof option for high-assurance contexts
- Applicable to all notification types

**9.3 Scope of Disclosure Risk Mitigation**

- Child/Youth: Low risk - minimal controls
- Community/Regional: Medium risk - proportionate notification
- National/International: High risk - enhanced security, frequent notification
- Universal risk framework across contexts

**9.4 CIR Publication Security**

- Public accessibility does not compromise confidentiality (no PII in CIR)
- CIR-ID verification prevents controller impersonation
- Registry-based validation enables cross-jurisdictional trust
- Rights access point provides secure channel for inquiries

**9.5 Co-Regulated Infrastructure Security**

- Independent receipt generation reduces single point of failure risk
- Public CIR registries enable regulatory verification at scale
- Transparency-by-default architecture resists surveillance
- Bilateral receipts provide audit trail for dispute resolution

---

## Section 10: Convention 108+ Digital Identification Transparency Profile

### 10.1 Treaty-Based Code of Conduct Framework

This profile positions **Council of Europe Convention 108+** as the normative legal framework governing digital identification transparency, rather than establishing a new code of conduct. The profile serves as the **technical implementation specification** for operationalizing Convention 108+ transparency requirements as digital public infrastructure.

**Rationale for Treaty-Centric Approach**:

1. **Legal Authority**: Convention 108+ is a ratifiable international treaty with binding enforcement via supervisory authorities (55+ jurisdictions)
2. **Existing "Must" Requirements**: Treaty already defines SHALL-level obligations (Articles 5, 8, 9, 10, 14)
3. **Longevity**: Treaties provide greater stability than voluntary codes of conduct

4. **Regulatory Coordination**: Supervisory authorities under Convention 108+ have established coordination mechanisms
5. **Universal Applicability**: Treaty applies horizontally across all legal bases and processing contexts

**What This Profile Adds**:

- **Technical operationalization** of Convention 108+ transparency requirements through notice receipts, CIRs, and Notice Event Logs
- **Digital identification conformance** for contexts where controller identification precedes individual identification
- **Risk-proportionate transparency** through scope of disclosure and TATA (Transparency and Trust Assurance) levels
- **Co-regulated infrastructure** enabling independent verification through public registries

**What This Profile Does NOT Do**:

- Does not create new legal obligations beyond Convention 108+
- Does not replace or contradict treaty requirements
- Does not establish governance authority (supervisory authorities retain oversight)

### 10.2 Convention 108+ Article Mapping

**Article 5 (Legitimacy and Proportionality)**:

- **Treaty Requirement**: "Personal data undergoing processing shall be: processed fairly and in a transparent manner"
- **Profile Implementation**: CIR publication enables transparency before processing begins; two-factor notice (2FN) provides bilateral proof
- **Field Mapping**: `controller_identity_record_id`, `cir_publication_url`, `two_factor_notice_indicator`

**Article 8(2) (Transparent Processing)**:

- **Treaty Requirement**: "The controller shall provide... at least information as to his or her identity, the legal basis and the purposes of the processing"
- **Profile Implementation**: CIR contains controller identity; notice receipt documents legal basis and purposes before processing
- **Field Mapping**: `party_id` (CIR-ID), `lawful_basis`, `processing_purposes`, `rights_access_point`
- **Operational Reference**: EU Regulation 2018/1725 Article 15 demonstrates Convention 108+ Article 8(2) implementation

**Article 9 (Rights of the Data Subject)**:

- **Treaty Requirement**: Rights of access, rectification, erasure, restriction, portability
- **Profile Implementation**: `rights_access_point` provides universal mechanism for exercising rights; Notice Event Log documents rights exercise events

- **Field Mapping**: `rights_access_point`, Notice Event Log `event_type` values (access_exercised, rectification_requested, erasure_requested)

**Article 10 (Additional Obligations)**:

- **Treaty Requirement**: "The controller... shall keep a register of processing operations under its responsibility"
- **Profile Implementation**: Notice Event Log provides append-only register of processing operations; CIR enables public controller registry
- **Field Mapping**: Notice Event Log structure, `notice_event_log_url`
- **Operational Reference**: EU Regulation 2018/1725 Article 31 (records of processing activities) demonstrates Convention 108+ Article 10 implementation with public central register (Article 31(5))

**Article 14 (Transborder Flows)**:

- **Treaty Requirement**: "A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation transborder flows of personal data... where [adequate safeguards exist]"
- **Profile Implementation**: `scope_of_disclosure`, `recipient_jurisdictions`, `surveillance_risks`, and `transfer_mechanism` fields enable informed consent and adequate safeguards disclosure
- **Field Mapping**: `scope_of_disclosure="international"`, `recipient_jurisdictions`, `transfer_mechanism`, `surveillance_risks`
- **Operational Reference**: EU Regulation 2018/1725 Article 68 demonstrates Convention 108+ Article 14 implementation

### 10.3 Digital Identification Code of Conduct

The `codes_of_conduct` field (ISO/IEC 27560:2025 WD clause 6.3.4.20) references this profile as the **technical implementation** of Convention 108+ transparency requirements for digital identification contexts.

**Structured Format**:

```
{
  "codes_of_conduct": {
    "legal_framework": "Council of Europe Convention 108+",
    "implementation_profile": "ISO/IEC 27560 Universal Notice Receipt Profile v1.0",
    "conformance_level": "Universal Notice Receipt",
    "tata_level": 2,
    "jurisdiction": "CA",
    "supervisory_authority": "https://www.priv.gc.ca"
  }
}
```

**Simple Format** (backward compatible):

```
{
  "codes_of_conduct": "Council of Europe Convention 108+ operationalized via ISO/IEC 27560 Universal Notice Receipt Profile v1.0"
}
```

**Conformance Levels**:

- **Universal Notice Receipt**: ANCR Exchange Stage 1 (mandatory)
- **Authorization Exchange**: Stage 1 + Stage 2 for consent/authorization contexts
- **Full Protocol**: Stages 1-4 including portable tokens

**TATA (Transparency and Trust Assurance) Levels**:

- **Level 1 (Self-Assertion)**: Controller publishes CIR; notice receipts optional
- **Level 2 (Registry Verification)**: CIR-ID registered with authoritative source (e.g., ICO Controller Registry)
- **Level 3 (Notarized Receipts)**: Cryptographic signatures on receipts via Transparency and Trust Assurance Officer (TTAO)
- **Level 4 (Physical Verification + Active State)**: Notarized receipts with physical identity verification and remote active state validation

**Supervisory Authority Coordination**:

Controllers operating under Convention 108+ specify their supervisory authority in the `codes_of_conduct` field, enabling:

- Cross-jurisdictional verification through authority coordination mechanisms
- Registry federation for international controller lookup
- Enforcement coordination for cross-border violations

### 10.4 ISO/IEC 29100 Privacy Framework Modernization: Principle 7 → Principle 1

#### Proposed Framework Modernization: Principle 7 Becomes Principle 1

This profile proposes that **ISO/IEC 29100 Principle 7 (Openness, Transparency and Notice) be moved to Principle 1** as the foundational principle for modernizing privacy frameworks. This single architectural change enables all other principles to become operationally verifiable, enforceable, and scalable.

- **Traditional implementation**: Transparency is one of eleven co-equal principles
- **Modernized implementation**: Transparency-by-default as prerequisite infrastructure
- **Rationale**: Without verifiable transparency, other principles cannot be effectively implemented or enforced. The EDPB Guidelines on Transparency under Regulation 2016/679 establish that "transparency is an overarching obligation under the GDPR applying to three central areas" and that "transparency is now included as a fundamental aspect of these principles."[1] The guidelines further confirm that "the transparency

requirements in the GDPR apply irrespective of the legal basis for processing and throughout the life cycle of processing."[1]

**When Principle 7 Becomes Principle 1**, the remaining principles can be implemented as follows:

1. **Principle 2 (Consent and Choice)**: CIR publication and notice receipts enable informed consent before processing begins
2. **Principle 3 (Purpose Legitimacy and Specification)**: Notice Event Log documents purpose at notice issuance, preventing scope creep
3. **Principle 4 (Collection Limitation)**: Anonymous-by-default architecture limits collection to what's explicitly authorized
4. **Principle 5 (Data Minimization)**: Controller-ID first approach inverts surveillance model, minimizing by default
5. **Principle 6 (Use, Retention and Disclosure Limitation)**: Notice Event Log tracks all changes to use, retention, disclosure scope
6. **Principle 7 (Accuracy and Quality)**: Rights access point enables rectification requests with bilateral proof
7. **Principle 8 (Openness, Transparency and Notice)**: **Becomes foundational as new Principle 1**, enabling all other principles through co-regulated infrastructure that makes transparency independently verifiable
8. **Principle 9 (Individual Participation and Access)**: Notice receipts provide portable proof for rights exercise
9. **Principle 10 (Accountability)**: Public CIR registries enable automated accountability verification at scale
10. **Principle 11 (Information Security)**: Bilateral receipts and Notice Event Log provide security through transparency

**Key Innovation**: By implementing transparency as **digital public infrastructure** through publicly accessible CIRs, standardized notice.txt files, and bilateral notice receipts, this profile demonstrates that transparency is not merely one principle among many—it is the **enabling infrastructure** that makes all other privacy principles operationally verifiable, enforceable, and scalable.

**Modernization Impact**:

- **From regulatory guidance to verifiable infrastructure**: EU Regulation 2018/1725 Article 15 (Information to be provided where personal data are collected) demonstrates Convention 108+ Article 8(2) transparency requirements operationally—this profile implements those requirements as independently verifiable digital public infrastructure through CIR publication and standardised notice receipts
- **From aspirational to operational**: Transforms ISO/IEC 29100 principles from compliance checklists into verifiable digital infrastructure

- **From controller-attestation to independent verification**: Public CIR registries enable regulatory oversight without requiring controller cooperation
- **From manual audits to automated enforcement**: Receipt verification scales through cryptographic proof and public registries

> **Note to Standards Body**: This profile proposes a single structural change to ISO/IEC 29100:2011—**moving Principle 7 (Transparency) to Principle 1**. This reordering does not modify principle definitions, but positions transparency as the enabling infrastructure that makes all other privacy principles operationally verifiable through the Universal Notice Receipt architecture.

### 10.2 Convention 108+ Alignment and Jurisdictional Implementation Examples

This profile uses **Council of Europe Convention 108+** as the authoritative international treaty framework for data protection transparency requirements. Convention 108+ is:

- Ratifiable as international treaty (eligible for treaty force 2026)
- Implemented by 55+ jurisdictions globally
- Technology-neutral and universally applicable

**EU Regulation 2018/1725** is referenced as the **best-practice operational implementation** of Convention 108+ transparency requirements, particularly:

- **Article 15**: Information to data subjects (implements Convention 108+ Article 8(2) transparent processing)
- **Article 31**: Records of processing activities, including requirement for **public central register** per Article 31(5) (implements Convention 108+ Article 10)
- **Article 39**: Data protection impact assessments (implements Convention 108+ proportionality principles)
- **Article 68**: Transfers of personal data to third countries (implements Convention 108+ Article 14)
- **Article 80**: Right of access by data subject to operational personal data (implements Convention 108+ Article 9 for operational contexts)
- **Article 88**: Logging requirements for operational personal data processing operations (implements Convention 108+ accountability principles)

**Convention 108+ to Profile Mapping**:

- **Article 8(2)**: Transparent processing → CIR publication requirement (notice.txt at /.well-known/transparency)
- **Article 9**: Rights of data subject → rights_access_point universal implementation
- **Article 14**: Cross-border flows → scope_of_disclosure risk determination + surveillance_risks disclosure
- **Article 31 (EU 2018/1725)**: Public central register → CIR registry infrastructure enabling co-regulated transparency

- **Article 80 (EU 2018/1725)**: Access to operational personal data → rights_access_point for lawful access contexts
- **Article 88 (EU 2018/1725)**: Logging of operational personal data operations → Notice Event Log specification
- **Horizontal transparency requirements** → universal notice receipt applicability across all legal bases

**Jurisdictional Implementation Examples** (Non-Normative):

Regional and national frameworks implementing Convention 108+ principles are acknowledged as jurisdictional examples:

- **GDPR (EU 2016/679)**: EU/EEA implementation with Articles 13-14 (information provision), Article 30 (records of processing), Article 49 (derogations for transfers)
- **PIPEDA (Canada)**: Principle 4.1.3 accountability, substantial similarity with Convention 108+ for adequacy determinations
- **Privacy Act 1988 (Australia)**: APP 8 (cross-border disclosure), APP 1 (open and transparent management)
- **Quebec Law 25**: Article 17 (transfers outside Quebec), enhanced consent and transparency requirements

These jurisdictional frameworks are **not normative** for this international profile. They serve as examples of how Convention 108+ principles are operationalized in different legal contexts.

### 10.3 ISO/IEC 29184:2020

- Appendix D references Kantara MVCR work (this profile completes that contribution)
- Clause 5.2.8: Ongoing reference → Notice Event Log implementation
- Clause 5.4: Consent management → Authorization Exchange Protocol (Part 2)
- Profile demonstrates MVCR completion beyond privacy-only scope

### 10.3 ISO/IEC 27701 (PIMS)

- CIR and notice receipts within PIMS scope
- Awareness and training SHALL include notice receipt concepts
- Applicable to controller accountability across contexts

### 10.4 W3C Data Privacy Vocabulary

- Field mappings SHOULD align with DPV terms for privacy contexts
- Enables semantic interoperability across systems
- Profile extends DPV applicability to non-privacy contexts

### 10.5 Related Standards Development

This profile supports and aligns with ongoing standards development:

- **ISO/IEC 27568** (Digital Twins): CIR and notice receipts applicable to digital twin privacy

- **ISO/IEC 27566** (Age Assurance): Scope of disclosure categories enable age-appropriate transparency
- **ISO/IEC 27091** (Gen AI Security & Privacy): Stage 4 portable tokens address AI agent authorization
- **IEEE P7012: Machine Readable Personal Privacy Terms standard enables automated processing of privacy terms, aligning with this profile's notice.txt machine-readable transparency requirements**
- **A Canadian National Consent Standard**: Profile provides international alignment

### 10.6 Trustmark Visual Signaling (Implementation-Neutral)

This profile specifies **Transparency and Trust Assurance (TATA)** levels as abstract assurance progression, enabling implementers to provide visual trustmark signaling without mandating specific designs.

**TATA Levels Signaling Requirements**:

Visual implementations MAY signal conformance through trustmarks displaying:

1. **Treaty Framework**: Convention 108+ compliance
2. **Implementation Profile**: ISO/IEC 27560 Universal Notice Receipt Profile v1.0
3. **Conformance Level**: Universal Notice Receipt / Authorization Exchange / Full Protocol
4. **TATA Level**: 1 (Self-Assertion), 2 (Registry Verification), 3 (Notarized Receipts), 4 (Physical Verification + Active State)

**Generic Text-Based Representation** (Example):

```
Convention 108+ Compliant | Digital Transparency by Default (L2) | ISO/IEC 27560 UNRP v1.0
```

**Structured Representation** (Machine-Readable):

```
{
  "trustmark": {
    "framework": "Convention 108+",
    "profile": "ISO/IEC 27560 UNRP v1.0",
    "conformance_level": "Universal Notice Receipt",
    "tata_level": 2,
    "verification_url": "https://registry.example/verify/CIR-CA-12345"
  }
}
```

**Visual Implementation Principles** (Non-Normative Guidance):

- **Implementation-neutral**: Profile does not mandate specific logos, colors, or visual designs

- **Recognizable at a glance**: Visual representation should enable rapid controller accountability verification
- **Risk-proportionate**: Higher TATA levels may warrant more prominent visual signaling
- **Verifiable**: Trustmark should link to verification mechanism (CIR registry, TTAO signature validation)

**Reference Implementations**:

Implementers developing trustmark visual systems are encouraged to publish their designs as reference implementations. This profile establishes the **semantic requirements** (what information trustmarks convey); visual designers establish **presentation standards** (how information is displayed).

> **Note**: This is noted for v1.1, which will address trustmark certification programs, visual standard coordination, and cross-implementation interoperability after base infrastructure adoption demonstrates market demand.

---

## Section 11: Implementation Guidance

### 11.1 For Controllers (All Contexts)

**Step 1: Structure and Publish CIR**

- Populate party fields with Controller role
- Generate CIR-ID (URI, DID, legal entity identifier)
- **Register with authoritative source** (e.g., ICO Controller Registry, OAIC, OPC)
- **Obtain registrar blind data notary signature** on CIR
- Publish signed CIR at /.well-known/transparency or equivalent public location (IETF application in progress)

**Independent Receipt Verification Flow (Level 2 - Registrar Blind Data Notary)**:

1. Individual generates receipt using public CIR + registrar signature
2. Any party validates receipt against registrar's public key (no controller involvement)
3. Registrar signature proves: CIR authenticity, registration timestamp, controller accountability
4. **Privacy-through-architecture**: Registrar signs CIR without accessing PII Principal identifiers in receipts

**Enhanced Assurance Flow (Level 3/4 - DTTO Physical Notarization)**:

For high-risk contexts (cross-border lawful interception, critical infrastructure, vital interest):

1. **DTT Certification**: Digital Transparency and Trust Officer undergoes physical identity verification and training
2. **Micro-Credential Notarization**: A Digital Privacy Officer physically notarizes ANCR Exchange Stage 3 micro-credentials to assure via face-to-face liveliness

3. **Cross-Border Dynamic Authorization**: DTTO-signed credentials enable real-time lawful access coordination across jurisdictions
4. **Active State Validation**: Level 4 adds remote attestation for real-time transparency state monitoring

**Step 2: Implement 2FN**

- Present CIR before any processing or interaction
- Generate notice receipt with unique notice_receipt_id
- Provide receipt to individual (display, download, API)
- Do NOT require pii_principal_id or any individual identifier in ANCR Exchange Stage 1

**Step 3: Maintain Notice Event Log**

- Log notice issuance, authorizations, material changes, rights exercises
- Make queryable via CIR rights access point
- Support cross-context queries (privacy, safety, security, environment)
- **For Level 3/4**: Log notarization events and active state validation checks

### 11.2 For Individuals

**Step 1: Retrieve CIR and Generate Notice Receipt**

- Access controller's public information to generate a CIR,
- Review CIR for controller identification and rights access (ANCR TPI-R)
- Generate notice receipt independently (or via controller presentation)
- Store notice receipt in personal data store or Consent capable digital authorisation wallet
- Note: no individual identifier required - remain anonymous by default

**Step 2: Monitor Notice Event Log**

- Check CIR rights access point for material changes
- Exercise rights via CIR contact information
- Use notice receipts for secondary purpose authorization (ANCR Exchange Stage 2)

### 11.3 For Regulators

**Adoption Pathway**:

1. Validate notice receipt architecture against Convention 108+ transparency requirements
2. Establish Controller 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. Establish notarial and public broadcast notice services

> **Note**: Kantara ANCR TPI-R is complementary to this profile. The profile defines **what** transparency infrastructure must exist. TPI-R defines **how** to verify it's operational.

---

### 11.4 Role Mapping for Transparency Project Implementation

**Fundamental Principle**: Roles in the Universal Notice Receipt Profile are **relative to the stakeholder holding the ANCR record**. The same entity may play different roles in different record contexts.

## 11.4.1 Role Determination Rule

**To map roles for any ANCR implementation:**

1. **Identify the record holder** (who holds this specific ANCR record?)
2. **Map record holder → PII Principal** (the holder is always the Principal for their own record)
3. **Map record issuer → Controller** (who issued/signed this record?)
4. **Map record verifiers → Third-Party Controllers** (who validates this record?)

## 11.4.2 Core ISO/IEC 29100 Roles

| ISO/IEC 29100 Role | Definition | ANCR Context |
|---|---|---|
| **PII Principal** | Individual who is the record holder for THIS specific ANCR record | Holds notice receipt; may or may not be the data subject |
| **PII Controller** | Entity that issued/signed the ANCR record; maintains CIR and Notice Event Log | Issues notice receipts; maintains transparency infrastructure |
| **Joint Controller** | Multiple controllers sharing responsibility for processing | Multiple CIR-IDs referenced in single notice receipt |
| **PII Processor** | Entity processing PII on behalf of controller | Referenced in notice receipt `processor` field |
| **Sub-Processor** | Processor engaged by primary processor | Nested processor reference in notice receipt |
| **Third-Party Controller** | Separate controller receiving data from original controller | Verifies ANCR Exchange Stage 3/4 credentials from original controller |

## 11.4.3 Verifiable Credentials Pattern Mapping (Perspective-Relative)

**When Individual holds credential from Controller:**

| VC/SSI Role | ISO/IEC 29100 Role | ANCR Context | Record Location |
|---|---|---|---|
| **Holder** | PII Principal | Individual holding notice receipt from Issuer | Principal's wallet/storage |
| **Issuer** | PII Controller | Entity that issued credential/receipt (maintains CIR) | Issuer's Notice Event Log |

| VC/SSI Role | ISO/IEC 29100 Role | ANCR Context | Record Location |
|---|---|---|---|
| **Verifier** | Third-Party Controller | Entity requesting credential presentation | Verifier's processing record |
| **Subject** | Data Subject | Individual whose attributes are in credential | N/A (attribute level) |

**Example Scenario: University Degree Credential**

**Alice's Perspective (Alice holds ANCR Stage 3 credential):**

- **Alice** = PII Principal (credential holder)
- **University** = PII Controller (issued degree credential, maintains CIR-UNIVERSITY-123)
- **Employer** = Third-Party Controller (verifies credential when Alice applies for job)
- **Alice** = Data Subject (her degree attributes are being verified)

**University's Perspective (University holds ANCR record from Accreditation Body):**

- **University** = PII Principal (holds accreditation credential)
- **Accreditation Body** = PII Controller (issued accreditation, maintains CIR-ACCREDIT-456)
- **Alice** = Verifier (checks University's CIR before enrolling)
- **University** = Data Subject (its accreditation status is being verified)

**Employer's Perspective (Employer holds ANCR record from Data Protection Authority):**

- **Employer** = PII Principal (holds compliance certificate)
- **Data Protection Authority** = PII Controller (issued certificate, maintains CIR-DPA-789)
- **Prospective Employees** = Verifiers (check Employer's CIR before applying)

### 11.4.4 ANCR Exchange Stage Role Progression

**Stage 1 (Notice Receipt): Controller → Principal**

- **Controller presents CIR** to Individual
- Individual = PII Principal (receives notice, holds receipt)
- Controller = PII Controller (issues notice, holds receipt copy)
- Bilateral proof: both hold synchronized receipt

**Stage 2 (Authorization): Principal → Controller**

- **Individual returns authorized receipt**
- Individual = PII Principal (grants authorization)
- Controller = PII Controller (receives authorization)
- Notice Event Log updated with authorization event

**Stage 3 (Credential Presentation): Principal → Verifier**

- **Individual presents credential** to Third Party

- Individual = PII Principal (credential holder)
- Original Controller = PII Controller (credential issuer, referenced in token)
- Third Party = Third-Party Controller (verifier, becomes new controller if processing PII)

**Stage 4 (Portable Token): Principal → Multiple Controllers**

- **Individual presents token** to any controller
- Individual = PII Principal (token holder, controls portability)
- Original Controller = PII Controller (maintains original Notice Event Log)
- Recipient Controllers = Third-Party Controllers (verify token, honor authorization)

## 11.4.5 Multi-Party Role Mapping Example

**Scenario**: Alice uses her health insurance credential to book a medical appointment.

**Alice's ANCR Record (Stage 4 Consent Token):**

```
Record Holder: Alice (PII Principal)
Issuer: Health Insurance Co. (PII Controller - maintains CIR-HEALTH-123)
Current Verifier: Medical Clinic (Third-Party Controller - checking coverage)
Original Subject: Alice (Data Subject - her health data)
```

**Health Insurance Co.'s ANCR Record (Stage 2 Authorization):**

```
Record Holder: Health Insurance Co. (PII Principal for THIS record)
Issuer: Medical Licensing Board (PII Controller - verifies insurance license)
Verifiers: Alice + Regulatory Authority (both verify insurance CIR)
```

**Medical Clinic's ANCR Record (Stage 1 Notice Receipt):**

```
Record Holder: Medical Clinic (PII Principal for THIS record)
Issuer: Data Protection Authority (PII Controller - issued compliance certificate)
Verifiers: Alice (verifies clinic's CIR before sharing health data)
```

## 11.4.6 Cross-Framework Role Equivalencies

| ISO/IEC 29100 Role | Convention 108+ Term | GDPR Term | PIPEDA Term | Quebec Law 25 Term |
|---|---|---|---|---|
| PII Principal | Data subject | Data subject | Individual | Personne concernée |
| PII Controller | Controller | Controller | Organization | Entreprise |
| PII Processor | Processor | Processor | Third party (service provider) | Sous-traitant |
| Third-Party Controller | Recipient controller | Third party / Joint controller | Third party | Tiers |

### 11.4.7 Implementation Pattern Examples

**Pattern 1: SSI/DID Architecture**

- Individual maintains DID as `principal_anchor`
- Controllers issue verifiable credentials bound to DID
- Individual presents credentials across multiple controllers
- **Role mapping**: Holder = PII Principal, Issuer = PII Controller, Verifier = Third-Party Controller

**Pattern 2: OAuth/UMA Authorization**

> **Note for Reviewers**: Detailed OAuth/UMA role mapping examples with authorization server, resource server, and client role mappings will be provided in v1.1 specification. OAuth/UMA patterns demonstrate how ANCR Exchange Stages 3-4 align with existing authorization infrastructure. Request v1.1 role mapping appendix materials for OAuth/UMA implementation guidance.

**Pattern 3: Federated Identity**

- Identity Provider issues ANCR Stage 1 (Notice Receipt) with authentication assertion
- Relying Party verifies assertion against IdP's CIR
- Individual remains PII Principal across federation
- **Role mapping**: Individual = PII Principal, IdP = PII Controller, Relying Party = Third-Party Controller

### 11.4.8 Role Mapping Anti-Patterns (What NOT to Do)

❌ **Anti-Pattern 1**: Assuming Controller is always the same entity across all records

- **Problem**: Alice is Principal when receiving University credential, but Controller when issuing authorization to Employer
- **Correct**: Map roles relative to each specific ANCR record

❌ **Anti-Pattern 2**: Mapping Holder → Controller

- **Problem**: In VC systems, Holder often has control, leading to incorrect mapping
- **Correct**: Holder → PII Principal (record recipient), Issuer → PII Controller (record creator)

❌ **Anti-Pattern 3**: Confusing Data Subject with PII Principal

- **Problem**: Data Subject is whose data is protected; PII Principal is who interacts with the record
- **Correct**: One person can be both, but roles are distinct (see Section 3.18-3.19)

❌ **Anti-Pattern 4**: Fixed role assignments across ANCR stages

- **Problem**: Assuming Controller in Stage 1 remains Controller in Stage 4
- **Correct**: Roles shift as record moves through stages—Principal becomes presenter, original Controller becomes referenced issuer

### 11.4.9 Implementation Guidance: Determining Your Role

**Step 1: Identify which ANCR record you're implementing**

- Are you the holder/recipient of a notice receipt?
- Are you issuing a notice receipt to someone else?
- Are you verifying a credential/token presented to you?

**Step 2: Map your role for THIS specific record**

- **You hold the record** → You are PII Principal (for this record)
- **You issued the record** → You are PII Controller (maintain CIR + Notice Event Log)
- **You verify the record** → You are Third-Party Controller (verify against CIR registry)

**Step 3: Identify other roles relative to YOUR position**

- Who gave you this record? → They are Controller (for this record)
- Who are you giving this record to? → They are Third-Party Controller (or individual verifier)
- Whose data is in this record? → They are Data Subject

**Step 4: Document role mapping in implementation**

- Record which ANCR stage you're implementing
- Document your role perspective clearly
- Reference CIR-IDs for all controller roles
- Update Notice Event Log with role-based events

---

> **Note for v1.1**: Detailed OAuth/UMA role mapping examples, authorization server patterns, and resource server role progressions will be standardized in v1.1. Reviewers requiring OAuth/UMA implementation guidance for v1.0 evaluation may request supplementary materials demonstrating ANCR Exchange Stage 3-4 alignment with RFC 6749, RFC 8693, and UMA 2.0 grant patterns.

---

# PART 2: AuthC EXCHANGE PROTOCOL

## Optional Extensions for Consent Portability and Agentic Coordination

### Section 12: Authorization Exchange Overview

#### 12.1 Addressing Base Standard Gap

ISO/IEC 27560:2025 does not specify exchange protocol for privacy receipts. This authorization exchange protocol defines:

- Exchange pattern: How receipts flow between parties across four stages

- Exchange semantics: What each stage authorizes
- Exchange structure: Field additions per stage
- Universal applicability: Same pattern across privacy, safety, security, environment contexts

### 12.2 Four-Stage Progression

**ANCR Exchange Stage 1 (Notice Receipt)**: Notice acknowledgment (bilateral proof)

**ANCR Exchange Stage 2 (Consent Notice Receipt)**: Explicit authorization (consent, contract, policy acceptance, etc.)

**ANCR Exchange Stage 3 (Micro Notice Credential)**: Technical context authorization (API, device, remote verification)

**ANCR Exchange Stage 4 (Consent Token)**: Individual-controlled authorization portability (agentic coordination, consent authorization in digital wallets)

---

## Section 13: ANCR Exchange Stage 2 - Consent Notice Receipt

### 13.1 Authorization Types by Context and Legal Basis

**Privacy Context Authorizations**:

**Consent**: authorization_type="consent_granted"

- consent_timestamp, consent_type, permissions_bundle, pii_principal_id (optional)
- Enables secondary purpose consent using existing ANCR Exchange Stage 1 notice receipt

**Contract**: authorization_type="contract_accepted"

- contract_timestamp, contract_terms_version, permissions_bundle

**Legal Obligation**: authorization_type="legal_access_acknowledged"

- legal_authority_reference, access_scope, access_timestamp

**Legitimate Interest**: authorization_type="legitimate_interest_objection"

- balancing_test_reference, opt_out_mechanism, objection_timestamp

**Vital Interest**: authorization_type="emergency_notified"

- emergency_justification, emergency_timestamp, post_facto_notification

**Public Interest**: authorization_type="public_interest_participation"

- ethics_board_reference, public_benefit_description, participation_timestamp

**Non-Privacy Context Authorizations**:

**Safety**: authorization_type="safety_acknowledgment"

- hazard_description, safety_measures_required, acknowledgment_timestamp

**Security**: authorization_type="security_policy_acceptance"

- policy_version, security_requirements, acceptance_timestamp

**Environment**: authorization_type="environmental_disclosure_acknowledgment"

- disclosure_scope, environmental_impact, acknowledgment_timestamp

**Complete specifications**: See Appendix B (Legal Bases and Context Implementation)

## Section 14: ANCR Exchange Stage 3 - Micro Notice Credential

### 14.1 Technical Context Authorization

**Field Additions**:

- cryptographic_signature: Signature over receipt + permissions
- credential_binding: Device ID, session ID, API key
- technical_permissions_scope: API endpoints, data operations
- validity_period: Credential expiration

**Use Cases**:

- API authorization with granular permissions
- Cross-device authorization synchronization
- Third-party Controller verification without full receipt sharing
- IoT device authorization for safety/security contexts

## Section 15: ANCR Exchange Stage 4 - Consent Token

### 15.1 Individual-Controlled Portability

**Field Additions**:

- principal_anchor: DID, public key, wallet address
- token_claims: Issuer, subject, audience, expiration
- cross_controller_metadata: Original CIR-ID, provenance
- portability_scope: Geographic, jurisdictional, purpose restrictions

**Use Cases**:

- Agentic coordination with consent authorization tokens
- Authorization consent wallet management (privacy, safety, security contexts)
- Directed authorization to third-party controllers
- Cross-jurisdictional authorization portability

## Section 16: Authorization Exchange Conformance

### 16.1 Conformance Levels

**Universal Notice Receipt Conformance**: ANCR Exchange Stage 1 (mandatory for all contexts)

**Authorization Exchange Conformance**: ANCR Exchange Stage 1 + Stage 2 for applicable contexts

**Full Protocol Conformance**: ANCR Exchange Stages 1-4 (technical credentials and portability)

### 16.2 Mandatory for Authorization Exchange

- ANCR Exchange Stage 2 support for contexts requiring explicit authorization
- Notice Event Log updates for authorization events
- Authorization withdrawal/termination mechanism

## Section 17: Token Security Considerations

### 17.1 Replay Attack Prevention

- Unique token identifiers (jti)
- Time-bound tokens with expiration
- Nonce-based challenge-response

### 17.2 Authorization Freshness Validation

- Token issuance must be after latest Notice Event Log material change
- Controllers reject tokens issued before policy updates

### 17.2.1 Active State Synchronic Validation (Level 4)

For TATA Level 4 (Active State + Physical Verification) implementations, consent tokens SHALL include cryptographic binding to the notice.txt (CIR) state at time of issuance:

**Synchronic Matching Requirement**:

- Consent tokens SHALL include cryptographic hash of notice.txt (CIR) at time of token issuance
- Token verification SHALL confirm that current notice.txt matches the hashed version included in token
- If controller updates notice.txt (material change to CIR), all previously issued tokens become invalid until individual re-authorizes against updated CIR
- Notice Event Log SHALL record CIR version hash with each token issuance event

**Security Benefits**:

1. **Prevents Stale Consent Exploits**: Tokens automatically invalidate when CIR changes, preventing controllers from relying on old authorizations after changing processing terms
2. **Prevents CIR Hijacking**: Attacker cannot serve fake notice.txt at unauthorized endpoint—token verification fails if CIR hash doesn't match registry-signed version
3. **Prevents Fake Hash Injection**: Token hash must match both current CIR AND Notice Event Log entry—controller cannot forge hash without registry detection
4. **Enables Real-Time Compliance**: Regulators verify token validity by comparing CIR hash against Notice Event Log without controller cooperation

**Implementation Pattern**:

```
{
  "token_claims": {
    "iss": "CIR-CA-12345",
    "jti": "receipt-abc-123",
    "iat": "2025-12-13T19:00:00-05:00",
    "exp": "2026-12-13T19:00:00-05:00",
    "cir_hash_at_issuance": "sha256:a1b2c3d4...",
    "cir_publication_url": "https://example.com/.well-known/transparency/notice.txt",
    "notice_event_log_verification_url": "https://registry.example.org/verify/CIR-CA-12345"
  }
}
```

**Verification Protocol**:

1. Extract `cir_hash_at_issuance` from token
2. Fetch current notice.txt from `cir_publication_url`
3. Compute hash of current notice.txt
4. Compare computed hash with `cir_hash_at_issuance`
5. If mismatch: Token invalid—CIR has been updated since token issuance
6. Query Notice Event Log to confirm `cir_hash_at_issuance` matches log entry at token `iat` timestamp
7. If log mismatch: Token invalid—hash was forged or CIR was hijacked

**Attack Prevention**:

**Attack 1: CIR Hijacking at Unauthorized Endpoint**

- Attacker serves fake notice.txt at compromised endpoint
- Token contains hash of legitimate CIR from registry
- Verification fails: fake notice.txt hash ≠ token `cir_hash_at_issuance`
- **Defense**: Cryptographic binding prevents acceptance of hijacked CIR

**Attack 2: Fake Hash Injection in Token**

- Attacker creates token with fake `cir_hash_at_issuance`
- Verification queries Notice Event Log for CIR hash at token `iat` timestamp
- Log hash ≠ token hash (registry signed log cannot be forged)
- **Defense**: Notice Event Log provides authoritative hash history—token rejected if hash doesn't match log

**Attack 3: Stale Consent After Material Change**

- Controller updates notice.txt (changes `scope_of_disclosure` from regional to international)
- Old tokens contain hash of pre-change CIR

- Verification computes hash of current notice.txt
- Current hash ≠ token `cir_hash_at_issuance`
- **Defense**: Automatic token invalidation forces re-authorization under new terms

**Regulatory Oversight**:

- Supervisory authorities verify token validity by:
  1. Retrieving token from data subject or controller
  2. Querying public Notice Event Log for CIR hash at token issuance time
  3. Comparing with current CIR hash
  4. Automated detection of tokens issued under outdated terms

> **Editorial Note for v1.1**: Active State Synchronic Validation will be standardized as mandatory for TATA Level 4 implementations in v1.1. Current v1.0 version documents the pattern as INFORMATIVE guidance for Level 4 implementers. V1.1 will specify: normative hash algorithm requirements (SHA-256 minimum), Notice Event Log CIR version tracking protocols, and cross-registry CIR hash verification standards for international token portability.

### 17.3 Revocation Mechanism

- Notice Event Log tracks revocation events
- Controllers maintain revocation list
- Real-time revocation check API

# APPENDICES

## Appendix A: Field Mapping to ISO/IEC 27560:2025

> **Complete field mapping**: 🗺️ Section 6.3: MVCR Field Mapping to Base ISO/IEC 27560:2023

> (Will be updated for universal context applications)

**Summary of Modifications for Universal Notice Receipt Profile**:

**Removed Fields**:

- pii_principal_id (ANCR Exchange Stage 1 only; optional Stage 2+)

**New Fields**:

- controller_identity_record_id (CIR-ID)
- cir_publication_url (public CIR location)
- notice_receipt_type (ANCR Exchange Stage 1-4)
- notice_type (notification, disclosure, policy, signal)

- context_category (privacy, safety, security, environment)
- two_factor_notice_indicator (boolean)
- scope_of_disclosure (risk category)
- permissions_bundle (granular permissions/authorizations)
- authorization_type (ANCR Exchange Stage 2 semantic variation)

**Enhanced Fields**:

- party_id → CIR-ID when party_role="Controller"
- event_type → universal context values (notice_issued, consent_granted, safety_acknowledged, etc.)
- processing_locations → scope_of_disclosure determination

---

# Appendix B: Legal Bases and Context Implementation

**Purpose**: Demonstrates universal notice receipt implementation across all Convention 108+ legal bases and non-privacy contexts.

## B.1 Consent (Privacy Context)

ANCR Exchange Stage 1 notice receipt + Stage 2 consent authorization enables secondary purpose consent

## B.2 Contract (Privacy Context)

**Standard Contract Flow:**

Individual-proffered terms pattern using ANCR Exchange Stage 1 + Stage 2

**Contract + Consent Flow (Two-Stage Authorization):**

When contractual processing requires separate consent for personal data processing:

**Stage 1: Initial Consent for Personal Data Processing**

- ANCR Exchange Stage 1: Notice Receipt for personal data processing
- ANCR Exchange Stage 2: Consent authorization (authorization_type="consent_granted")
- Legal basis: **Consent** for collection and processing of personal data
- Purpose: Enable contractual relationship through personal data provision
- Notice Event Log records: consent_granted for personal data processing

**Stage 2: Contract Acceptance with Secondary Purpose**

- ANCR Exchange Stage 1: Notice Receipt for contractual terms (references first consent receipt)
- ANCR Exchange Stage 2: Contract authorization (authorization_type="contract_accepted")
- Legal basis: **Contract** for service delivery using consented personal data

- Purpose: Contractual obligations and service provision
- Notice Event Log records: contract_accepted referencing prior consent_granted
- consent_receipt_chain: Links to Stage 1 consent receipt ID

**Use Cases:**

- Financial services requiring consent for data collection before contract execution
- Employment contracts separating personal data consent from contractual obligations
- Service agreements where data processing requires separate consent authorization
- Contexts requiring explicit consent for identification before contractual relationship

**Field Requirements for Two-Stage Flow:**

```
{
  "authorization_type": "contract_accepted",
  "contract_timestamp": "2025-12-11T11:00:00Z",
  "contract_terms_version": "v2.0",
  "permissions_bundle": ["service_delivery", "contractual_obligations"],
  "prerequisite_consent_receipt_id": "consent_receipt_xyz_123",
  "consent_receipt_chain": ["consent_receipt_xyz_123"],
  "lawful_basis_primary": "contract",
  "lawful_basis_prerequisite": "consent"
}
```

**Notice Event Log Entries:**

1. Stage 1: `consent_granted` for personal data processing
2. Stage 2: `contract_accepted` with reference to prerequisite consent
3. Material changes to either consent or contract trigger new notice receipts

## B.3 Legal Obligation (Privacy Context)

Regulatory transparency enforcement with ANCR Exchange Stage 1 + optional Stage 3

## B.4 Legitimate Interest (Privacy Context)

Balancing test transparency with opt-out mechanism

## B.5 Vital Interest (Privacy Context)

Emergency authority coordination with post-facto notification

## B.6 Public Interest (Privacy Context)

Research, journalism, archiving transparency

## B.7 Legal Access (Privacy Context - Warrant Tokens)

Constitutional compliance with lawful access documentation

### B.8 Safety Contexts

Product recalls, hazard warnings, emergency notifications, providence, supply chain

### B.9 Security Contexts

Acceptable use policies, incident disclosures, access control

### B.10 Environment Contexts

Environmental impact disclosures, sustainability reporting

## Appendix C: Rights Access by Context

**Privacy Rights** (accessible by legal basis):

### C.1 Privacy Rights Controls Matrix

The following table documents all privacy rights and derivative digital transparency controls operationalized by this profile:

| Privacy Right | Legal Basis Context | Convention 108+ Article | Required in v1.0 |
|---|---|---|---|
| **Derivative Digital Transparency Controls** | | | |
| Controller-ID Before Inference | All Bases | Article 8 + 9 | ✅ YES |
| Scope of Disclosure Transparency | All Bases | Article 9 + 14 | ✅ YES |
| Digital Surveillance Risk Disclosure | All Bases | Article 14.2 + 11.3 | ✅ YES |
| Bilateral Notice Proof (2FN) | All Bases | Article 8 + 12 | ✅ YES |
| Notice Event Log Access | All Bases | Article 8 + 9 + EU 2018/1725 Art. 88 | ✅ YES |
| Autonomous Consent Withdrawal | Consent | Article 9 + 8 | ✅ YES |
| Active State Transparency | All Bases | Article 8 + 9 | ⚠️ Optional (TATA L4) |
| Notice of Derogation to Digital Surveillance Rights | Consent | Article 11.3 + 8 + 5.2 | ✅ YES |
| **Traditional Data Protection Rights** | | | |
| Right to Be Informed | All Bases | Article 8 | ✅ YES |
| Right to Access | All Bases | Article 9 | ✅ YES |
| Right to Rectification | All Bases | Article 9 | ✅ YES |
| Right to Erasure | Consent | Article 9 | ✅ YES |
| Right to Withdraw Consent | Consent | Article 5 | ✅ YES |
| Right to Data Portability | Consent | Article 9 | ✅ YES |

| Privacy Right | Legal Basis Context | Convention 108+ Article | Required in v1.0 |
|---|---|---|---|
| Right to Restrict Processing | All Bases | Article 9 | ⚠️ Optional |
| Right to Object | Legitimate Interest | Article 9 | ⚠️ Optional |

**Note**: Complete Privacy Rights Controls Matrix with field dependencies, implementation requirements, and testing criteria is maintained in the profile's supporting materials repository.

## C.2 Rights Access by Legal Basis

**Privacy Rights** (accessible by legal basis):

- Consent: Access, Rectification, Erasure, Portability, Withdraw Consent, Object
- Contract: Access, Rectification, Portability
- Legal Obligation: Access, Rectification (limited)
- Legitimate Interest: Access, Object, Rectification
- Vital Interest: Access (post-emergency)
- Public Interest: Access, Rectification (limited)

**Safety Rights**:

- Acknowledgment status verification
- Recall update notifications
- Hazard mitigation information access

**Security Rights**:

- Policy version access
- Security requirement clarification
- Access control rule verification
- Active Legal Status

**Environment Rights**:

- Disclosure detail access
- Impact assessment review
- Sustainability metric verification
- Environmental cost

**Access Point**: All rights exercised via CIR rights_access_point (universal across contexts)

# Appendix D: Emergency Protocols

**Break-the-Glass Scenario** (Privacy Context):

1. Generate emergency notice receipt with emergency_justification

2. Log emergency access in Notice Event Log
3. Post-facto notification when legally permitted
4. Provide 2FN reuired receipt for right to object or request erasure post-emergency

**Regulatory Logging**: Controllers log emergency access per jurisdiction requirements (e.g., 72 hours)

**Non-Privacy Emergency Scenarios**:

- Safety: Immediate hazard notification with post-facto receipt issuance
- Security: Incident response with contemporaneous or post-facto notification
- Environment: Environmental incident disclosure with regulatory notification

# Appendix K (Informative): Enhanced Transparency Features for v1.1

**Status**: INFORMATIVE — This appendix documents advanced features deferred from v1.0 for future standardization. None of these features affect v1.0 conformance.

## K.1 Privacy Preference Signals

**Deferred Rationale**: GPC integration and preference indicator infrastructure add implementation complexity beyond v1.0's core bilateral receipt architecture.

**Proposed v1.1 Specification**:

When `scope_of_disclosure` includes processing subject to user preference signals, the following fields enable preference integration:

### K.1.1 privacy_preference_signals Object

```
{
  "privacy_preference_signals": {
    "gpc_honored": true,
    "gpc_scope": ["analytics", "third_party_disclosure"],
    "dnt_recognized": false,
    "preference_center_url": "https://example.com/privacy-preferences",
    "preference_binding": "browser_signal"
  }
}
```

**Field Definitions**:

- **gpc_honored** (boolean): Whether W3C Global Privacy Control signal is respected
- **gpc_scope** (array): Processing categories affected by GPC (e.g., analytics, marketing, third_party_disclosure)
- **dnt_recognized** (boolean): Whether Do Not Track signal is recognized
- **preference_center_url** (string): URL where individuals can manage preferences

- **preference_binding** (enum): How preferences are enforced—"browser_signal", "receipt_anchored", "account_based"

**Integration with Notice Event Log**:

- Log preference signal changes with `event_type="preference_signal_received"`
- Record preference enforcement with `event_type="processing_restricted_by_preference"`

**Standards Alignment**:

- W3C Global Privacy Control specification
- IEEE P7012 Machine Readable Personal Privacy Terms
- Integration with `permissions_bundle` for preference-based permission gating

---

## K.2 Transparency Assurance and Trust Assurance Indicators

**Deferred Rationale**: TATA Indicator level visual signaling and trustmark infrastructure requires coordinated implementation across registries, TTAOs, and visual standard bodies.

**Proposed v1.1 Specification**:

#### K.2.1 transparency_assurance_level Field

Maps CIR to Four-Level TATA framework:

```
{
  "transparency_assurance_level": 2,
  "tata_description": "Registry Verification—CIR-ID registered with authoritative source",
  "registry_verification_url": "https://ico.org.uk/controller-registry/CIR-CA-12345",
  "last_verification_date": "2025-12-01"
}
```

**TATA Levels** (from Section 5.4 editorial note):

- **Level 1**: Self-Assertion (no registry; suitable for local/child scope)
- **Level 2**: Registry Verification (CIR-ID + Notice Event Log registered)
- **Level 3**: Notarized Receipts via Blind Data Notary (TTAO-signed credentials)
- **Level 4**: Physical Verification + Active State (in-person verification + real-time validation)

#### K.2.2 trustmark_certifications Array

```
{
  "trustmark_certifications": [
    {
      "trustmark_type": "habni_active_state",
      "certification_body": "Digital Transparency Lab",
      "certification_date": "2025-11-15",
      "verification_url": "https://transparencylab.ca/verify/habni-12345"
    },
    {
      "trustmark_type": "tpi_r_score",
      "score": 87,
      "assessment_date": "2025-11-20",
      "report_url": "https://transparencylab.ca/tpi-r/CIR-CA-12345"
    }
  ]
}
```

#### K.2.3 visual_trust_indicator Object

```
{
  "visual_trust_indicator": {
    "display_text": "Convention 108+ Compliant | Transparency-by-Default (L2)",
    "badge_url": "https://transparencylab.ca/badges/convention108-L2.svg",
    "verification_link": "https://ico.org.uk/controller-registry/CIR-CA-12345"
  }
}
```

**V1.1 Development Requirements**:

- Registry authority coordination protocols
- TTAO certification standards
- Blind data notary signature specifications
- Active state validation mechanisms
- Cross-implementation trustmark interoperability

---

## K.3 Global Privacy Rights Controls (GPRC)

**Deferred Rationale**: GPRC framework addressing 72 transparency contexts (3 vectors × 4 TATA levels × 6 legal bases) extends beyond v1.0's universal notice receipt base.

**Proposed v1.1 Specification**:

#### K.3.1 GPRC Architecture

Enables context-aware rights controls to exercise across all transparency contexts maintained through Notice Event Logs.  Provides for human consent withdrawal to multiple source in context with one decentralised command, imitating human control of privacy 8n physical space.

#### K.3.2 global_privacy_rights_controls Array

```
{
  "global_privacy_rights_controls": [
    {
      "context_id": "consent_L2_regional",
      "data_control_vector": "co_regulation",
      "tata_level": 2,
      "legal_basis": "consent",
      "scope_of_disclosure": "regional",
      "rights_available": ["access", "rectification", "erasure", "portability", "withdraw_consent", "object"],
      "rights_exercise_mechanisms": {
        "access": {
          "method": "api",
          "endpoint": "https://api.example.com/rights/access",
          "authentication_required": false,
          "response_time": "P30D"
        },
        "withdraw_consent": {
          "method": "notice_receipt_anchored",
          "mechanism": "Update Notice Event Log via rights_access_point",
          "authentication_required": false,
          "immediate_effect": true
        }
      }
    },
    {
      "context_id": "legitimate_interest_L3_international",
      "data_control_vector": "data_protection",
      "tata_level": 3,
      "legal_basis": "legitimate_interest",
      "scope_of_disclosure": "international",
      "rights_available": ["access", "object", "rectification"],
      "rights_exercise_mechanisms": {
        "object": {
          "method": "web_form",
          "url": "https://example.com/object-to-processing",
          "authentication_required": true,
          "balancing_test_disclosure": "https://example.com/legitimate-interest-assessment",
          "response_time": "P30D"
        }
      }
    }
  ]
}
```

### K.3.3 Context-Specific Rights Exercise

GPRC enables:

- **Automated Rights APIs**: Machine-readable rights exercise endpoints per context

- **Preference Signal Integration**: GPC triggers automatic objection in legitimate interest contexts
- **Notice Receipt Anchored Rights**: Withdraw consent by updating Notice Event Log without authentication
- **Regulatory Verification**: Supervisory authorities query rights availability across all contexts

**K.3.4 72 Digital Transparency Control Contexts**

3 Data Control Vectors:

1. **Personal Control (SSI/DID)**: Individual-controlled identifiers and credentials
2. **Data Protection (Federated ID)**: Controller-centric with regulatory oversight
3. **Co-Regulation (MVCR-ANCR)**: Bilateral receipts with public CIR registries

4 TATA Levels (per K.2.1)

6 Legal Bases (Convention 108+):

- Consent, Contract, Legal Obligation, Legitimate Interest, Vital Interest, Public Interest

**V1.1 Development Requirements**:

- Context-specific rights mapping across all 72 combinations
- API specification for automated rights exercise
- Integration with preference signals for rights triggering
- Regulatory oversight protocols for rights verification at scale

## K.4 V1.1 Implementation Timeline

**Phase 1 (Q1 2026)**: Privacy preference signal pilot implementations

**Phase 2 (Q2 2026)**: TATA Level 3 blind data notary protocols

**Phase 3 (Q3 2026)**: GPRC framework with automated rights APIs

**Phase 4 (Q4 2026)**: Full v1.1 specification with all enhancements integrated

# Appendix E: Open Questions for Reviewers

## Comments for Reviewers: Article 80 and Article 88 References

**Operational Personal Data Logging and Access Rights**

This profile references **EU Regulation 2018/1725 Articles 80 and 88** as the operational implementation of Convention 108+ transparency requirements for **operational personal data** contexts (law enforcement, national security, public security processing by EU institutions):

**Article 80 (Right of Access by the Data Subject)**:

- Data subjects have the right to access their operational personal data and related information

- Access may be restricted to protect investigations, public security, or rights of others
- This profile implements Article 80 through the universal `rights_access_point` field in the CIR, enabling rights exercise across all legal bases and contexts

**Article 88 (Logging)**:

- Controllers must keep logs for processing operations in automated processing systems: collection, alteration, access, consultation, disclosure (including transfers), combination, and erasure
- Logs must establish justification, date/time, identification of who consulted/disclosed data, and recipient identity
- Logs available to data protection officer and European Data Protection Supervisor on request
- This profile implements Article 88 through the **Notice Event Log** specification (Sections 5.6, 6.2, 7.1), which provides append-only audit trail across all contexts (privacy, safety, security, environment)

**Distinction from Lawful Access/Surveillance**:

- **Operational personal data** (Articles 80/88) = Data processing by EU institutions for security/law enforcement tasks
- **Lawful access/interception** = Government surveillance powers (foreign intelligence, wiretapping) disclosed via `surveillance_risks` field (Section 6.1.1.3)
- This profile addresses **both** operational personal data (through Notice Event Log and rights_access_point) **and** lawful access contexts (through Legal Obligation legal basis, surveillance_risks disclosure, and break-the-glass scenarios in Appendix D)

**Reviewer Consideration:**

Does the Notice Event Log specification adequately address Article 88 logging requirements for operational personal data contexts while remaining applicable across all universal contexts (privacy, safety, security, environment)?

---

## Comments for Reviewers: PII Principal Jurisdiction Field

**New Field Addition: pii_principal_jurisdiction (Section 6.1.1.5)**

This profile adds **pii_principal_jurisdiction** as an optional field in ANCR Exchange Stage 2+ to enable risk-appropriate cross-border transfer transparency. This field was not in the original scope but emerged as necessary during cross-border transfer specification development.

**Rationale for Addition:**

1. **Risk-Proportionate Disclosure**: Surveillance risks affect individuals differently based on their jurisdiction (e.g., FISA Section 702 applies to non-US persons; Schrems II adequacy applies to EU/EEA residents)
2. **Informed Consent**: Tailoring surveillance risk disclosure to individual's legal context enables truly informed consent for cross-border transfers

3. **Jurisdictional Rights**: Identifying applicable data protection framework (GDPR for EU, PIPEDA for CA, etc.) enables proper rights exercise
4. **Adequacy Assessment**: Transfer risk assessment requires knowing both source (PII Principal) and destination (recipient) jurisdictions

**Privacy-Preserving Implementation:**

- **NOT collected in Stage 1** to preserve anonymous-by-default architecture
- **Conditional in Stage 2+**: Only when `scope_of_disclosure="national"` or `"international"`
- **Determination method disclosure**: Controllers must disclose how jurisdiction was determined (self-declared, IP geolocation, account registration, etc.)
- **Accuracy and correction**: Individuals can correct if determination is inaccurate

**Reviewer Considerations:**

1. Does the conditional collection (Stage 2+ only, cross-border contexts only) appropriately balance transparency needs with privacy preservation?
2. Should determination method disclosure be mandatory to ensure individuals understand inference accuracy limitations?
3. Is ISO 3166-1 alpha-2 (country) and ISO 3166-2 (subdivision) the appropriate granularity standard?
4. Should the field be **recommended** vs. **optional** when `transfer_mechanism="consent"` to ensure informed consent?

**Alternative Approaches Considered:**

- **Generic disclosure only**: Describe surveillance risks without individual-specific tailoring (rejected: less informed consent)
- **Controller jurisdiction proxy**: Assume individual is in same jurisdiction as controller (rejected: inaccurate for international services)
- **Post-hoc determination**: Determine jurisdiction only when individual exercises rights (rejected: too late for informed consent)

This field strengthens cross-border transfer transparency while maintaining Stage 1 anonymity. Feedback welcome on implementation approach and privacy-preservation balance.

---

## Comments for Reviewers: Normative Reference Strategy

#### GDPR Replaced with Convention 108+ and EU Regulation 2018/1725

---

# Appendix G: Backward Compatibility with ISO/IEC TS 27560:2023

**Purpose**: Provides migration guidance for implementations based on freely accessible ISO/IEC TS 27560:2023 to Universal Notice Receipt Profile targeting ISO/IEC 27560:2025.

## G.1 Terminology Evolution

| Universal Notice Receipt Term | 2025 WD Term | 2023 TS Term | Notes |
|---|---|---|---|
| Notice receipt (universal) | Privacy receipt | Consent receipt | 2023 scope limited to consent only |
| Notice record (universal) | PII processing record | Consent record | 2023 scope limited to consent only |
| authorization_type | (implicit in lawful_basis) | N/A | New field for multi-basis and multi-context |
| notice_type | N/A | N/A | New field for context categorization |
| context_category | N/A | N/A | New field for domain categorization |
| Controller-ID Notice Receipt | N/A | N/A | Completes original MVCR purpose |
| Co-regulated infrastructure | N/A | N/A | Independent receipt generation capability |

## G.2 Field Migration

| 2023 TS Field | 2023 Clause | Universal Notice Receipt Field | Migration Action |
|---|---|---|---|
| record_id | 6.3.3.2 | receipt_id | Rename for semantic clarity |
| pii_principal_id | 6.3.3.1 | pii_principal_id | Make optional in Stage 1 |
| party_id (Controller) | 6.3.6.2 | controller_identity_record_id | Enhance with public registry verification |
| Update to "27560-COMMON-NOTICE-2025-1.0" | | | |
| (none) | N/A | cir_publication_url | Add public CIR location |
| (none) | N/A | notice_type | Add for context categorization |
| (none) | N/A | context_category | Add for domain categorization |
| (none) | N/A | authorization_type | Add for Stage 2 multi-basis/context support |
| (none) | N/A | scope_of_disclosure | Add for risk-proportionate transparency |
| (none) | N/A | two_factor_notice_indicator | Add for 2FN pattern |

## G.3 Migration Strategy

**For 2023 TS Implementers**:

1. Current 2023 TS consent record implementations remain valid
2. Adopt ANCR Exchange Stage 1 (Notice Receipt) as enhancement
3. Publish CIR at public location (/.well-known/transparency)
4. Maintain 2023 field compatibility while adding universal extensions
5. When 2025 IS publishes, adopt full multi-basis and multi-context support
6. Implement directly against 2025 WD with Universal Notice Receipt Profile
7. Use G.2 table for 2023 TS interoperability if needed
8. Deploy with confidence that 2023 systems can exchange receipts
9. Enable co-regulated infrastructure through public CIR publication

- Universal notice receipts (ANCR Exchange Stage 1) can be exchanged with 2023 TS systems
- schema_version field enables version detection
- 2023 systems interpret universal notice receipts as consent receipts (ignore new fields)
- Universal notice receipt systems read 2023 receipts and map to ANCR Exchange Stage 2 consent context

**2023 TS Conformance**: Base consent record per published specification

**Universal Notice Receipt Bridge**: 2023 TS fields + ANCR Exchange Stage 1 (Notice Receipt) + public CIR

**Universal Notice Receipt Full**: 2025 WD fields + ANCR Exchange Stage 1 + multi-basis/context Stage 2 support

**Authorization Exchange Extended**: Universal Notice Receipt Full + ANCR Exchange Stage 3-4 portability

- **Completion of MVCR purpose**: Universal notice receipt infrastructure applicable beyond privacy contexts
- **Early adoption**: Implementers using 2023 TS can adopt universal architecture now
- **Seamless migration**: Clear path when 2025 IS publishes
- **Interoperability**: 2023 and 2025 implementations can exchange receipts
- **Co-regulated infrastructure**: Independent receipt generation using public controller information
- **Transparency-by-default**: Controller accountability precedes individual identification
- **Universal applicability**: Same base requirements across safety, security, environment, privacy

Appendix G ensures existing 2023 deployments can adopt universal notice receipt architecture incrementally without breaking changes, while positioning for 2025 multi-basis and multi-context architecture.

# Appendix H: Profile Types for ISO/IEC 27560:2025

**Purpose**: This appendix positions the Co-Regulated Digital Privacy Profile within a family of three complementary profile types, each implementing different control models for PII processing transparency.

## H.1 Overview of Profile Types

ISO/IEC 27560:2025 PII Processing Record structure can support three distinct control models:

**Profile Type 1: Data Protection Privacy Receipt Profile**

- **Control Model**: Controller-centric (User-ID first)
- **Receipt Timing**: After individual creates account and provides PII
- **Trust Model**: Individual depends on controller promises
- **Architecture**: Centralized (tick box consent, privacy policies)
- **Primary Use**: Traditional data protection compliance (GDPR, regional frameworks)

**Profile Type 2: Co-Regulated Digital Privacy Profile** (This Document)

- **Control Model**: Co-regulated transparency (Controller-ID first)
- **Receipt Timing**: Before any PII processing or collection begins
- **Trust Model**: Verifiable through cryptographic receipts and public registries
- **Architecture**: Distributed (bilateral receipts, Notice Event Logs, glass-boxed)
- **Primary Use**: Transparency-by-default, Convention 108+ horizontal requirements

**Profile Type 3: Personal Data Control Profile**

- **Control Model**: Individual-controlled (SSI/DID anchored)
- **Receipt Timing**: Individual presents verifiable credentials on demand
- **Trust Model**: Individual controls authorization distribution
- **Architecture**: Decentralized (portable tokens, consent wallets, agentic coordination)
- **Primary Use**: Cross-controller portability, AI authorization, personal data sovereignty

## H.2 Architectural Comparison

| Aspect | Type 1: Data Protection | Type 2: Co-Regulated (This Profile) | Type 3: Personal Control |
|---|---|---|---|
| **Primary Identifier** | pii_principal_id (required in header) | controller_identity_record_id (CIR-ID first; pii_principal_id optional Stage 2+) | principal_anchor (DID, public key; individual-controlled) |
| **Receipt Issuance** | Controller issues after account creation | Bilateral generation at notice presentation (controller or individual can initiate) | Individual presents credential; controller verifies |

| **Aspect** | **Type 1: Data Protection** | **Type 2: Co-Regulated** (This Profile) | **Type 3: Personal Control** |
|---|---|---|---|
| **Notice Timing** | After individual provides PII | Before any PII collection (Controller-ID first) | Individual controls timing through credential presentation |
| **Transparency Mechanism** | Privacy policies (lengthy, rarely read) | Public standard notice.txt at /.well-known/transparency + Notice Event Log | Verifiable credentials with selective disclosure |
| **Trust Model** | Controller self-attestation | Cryptographic receipts + public CIR registries | Cryptographic proofs under individual control |
| **Security Model** | Centralized database (honeypot risk) | Distributed bilateral receipts (no central target) | Decentralized credentials (individual holds keys) |
| **Violation Detection** | Manual investigation after harm | Real-time automated verification through receipt validation | Individual-initiated verification on demand |
| **Revocation** | Requires controller cooperation | Immediate via Notice Event Log update | Individual revokes credential; controller loses access |
| **Cross-Controller Portability** | No portability | Receipt chain enables third-party disclosure tracking | Portable tokens enable cross-controller authorization |
| **Regulatory Oversight** | Manual audits (cannot scale) | Automated receipt verification via public CIR registries | Individual provides audit trail on demand |

## H.3 Use Case Alignment

**Profile Type 1 (Data Protection) Best For:**

- Organizations with existing GDPR compliance infrastructure
- Contexts where controller-centric record keeping is regulatory requirement
- Legacy systems transitioning to receipt-based transparency
- Jurisdictions without public transparency infrastructure

**Profile Type 2 (Co-Regulated) Best For:** (This Profile)

- Organizations implementing transparency-by-default
- Contexts requiring verifiable controller accountability before processing
- Jurisdictions with Convention 108+ horizontal transparency requirements
- Glass-Boxed Model implementations (security through transparency)
- Multi-stakeholder environments (education, healthcare, public services)
- Regulatory frameworks enabling independent receipt verification

**Profile Type 3 (Personal Control) Best For:**

- Agentic AI authorization scenarios

- Cross-controller consent portability requirements
- Individual-controlled consent wallets
- SSI/DID infrastructure deployments
- Contexts requiring maximum individual sovereignty
- Future-facing personal data sovereignty frameworks

## H.4 Profile Interoperability

**ANCR Exchange Stage 1-4 Progression Works Across All Profiles:**

All three profile types use the same **PART 2: Authorization Exchange Protocol** (Sections 12-17), enabling interoperability with human ettiquette:

**ANCR Exchange Stage 1 (Notice Receipt)**: Notice acknowledgment (profile-specific implementation)

- Type 1: Privacy receipt with pii_principal_id
- Type 2: Notice Receipt (anonymous-by-default)
- Type 3: Individual presents verifiable credential

**ANCR Exchange Stage 2 (Consent Notice Receipt)**: Authorization grant (universal across profiles)

- authorization_type varies by legal basis and context
- permissions_bundle documents granular authorizations

**ANCR Exchange Stage 3 (Micro Notice Credential)**: Technical credentials (universal across profiles)

- Cryptographic signatures for API/device authorization
- credential_binding for technical context

**ANCR Exchange Stage 4 (Consent Token)**: Portable tokens (universal across profiles)

- principal_anchor enables cross-controller portability
- token_claims provide verifiable authorization proof

**Migration Paths:**

**Type 1 → Type 2**: Organizations adopt public CIR publication, enable bilateral receipt generation

**Type 2 → Type 3**: Individuals anchor receipts to personal DIDs, enable portable tokens

**Type 1 → Type 3**: Direct migration through ANCR Exchange Stage 4 (Consent Token) adoption

## H.5 Convention 108+ Implementation Architecture

The **Co-Regulated Digital Privacy Profile (Type 2)** operationalizes Convention 108+ transparency requirements through three complementary implementation patterns, four risk-proportionate assurance levels, and support for all six legal bases.

**Three Control Implementation Patterns** (Convention 108+ Article 5 compliance):

1. **Personal Control (SSI/DID)** → Profile Type 3
    - Individual-controlled identifiers per Article 9 (data subject rights)
    - Implements Article 5.2 (informed consent through self-sovereign credentials)
2. **Data Protection (Federated ID)** → Profile Type 1
    - Controller-centric with regulatory oversight per Article 10 (accountability)
    - Implements Article 8.2 (transparent processing through privacy policies)
3. **Co-Regulation (Bilateral Receipts)** → Profile Type 2 (This Document)
    - Bilateral transparency infrastructure per Article 12 (mutual assistance)
    - Implements Article 8.2 (transparent processing through CIR registries and notice receipts)

**Four Levels of Transparency and Trust Assurance (TATA)** (Convention 108+ Article 9 proportionality):

- **Level 1 (Self-Assertion)**: Controller publishes notice.txt; suitable for local/child scope per Article 5.3 (proportionate to legitimate purpose)
- **Level 2 (Registry Verification)**: CIR-ID registered with authoritative source per Article 10 (records of processing); EU Regulation 2018/1725 Article 31(5) public central register model
- **Level 3 (Cryptographic Signatures)**: Blind data notary attestation per Article 8.2 (transparent processing in intelligible form)
- **Level 4 (Active State + Physical Verification)**: Real-time validation per Article 9 (proportionate to high-risk contexts); EU Regulation 2018/1725 Article 80 (operational personal data access)

**Six Legal Bases (Convention 108+ Article 5)**:

All profile types support all six Convention 108+ legal bases through Stage 2 `authorization_type` field:

- Consent (Article 5.2)
- Contract (Article 5.3.a)
- Legal Obligation (Article 5.3.b)
- Legitimate Interest (Article 5.3.c with balancing test)
- Vital Interest (Article 5.3.d)
- Public Interest (Article 5.3.e)

**Implementation Result**: 3 control patterns × 4 TATA levels × 6 legal bases = **72 distinct transparency implementation contexts** maintained through Notice Event Logs per Article 10 (records of processing operations) and EU Regulation 2018/1725 Article 88 (logging requirements).

### H.6 Standards Body Considerations

**This Profile's Positioning:**

The Co-Regulated Digital Privacy Profile (Type 2) extends ISO/IEC 27560:2025 base standard while maintaining field-level compatibility. Key innovations:

1. **Controller-ID First**: Inverts base standard assumption (record after permission → notice before processing)
2. **Anonymous-by-Default**: Removes pii_principal_id from ANCR Exchange Stage 1 (enables surveillance-resistant architecture)
3. **Bilateral Receipts**: Both controller and individual hold synchronized proof (enables glass-boxed transparency)
4. **Notice Event Log**: Append-only audit trail of all transparency state changes (enables automated oversight)
5. **Co-Regulated Infrastructure**: Independent receipt generation using public CIR (enables regulatory scalability)

**Relationship to Other Profiles:**

- **Does not replace Type 1**: Organizations can continue data protection approach
- **Enables progression to Type 3**: Provides bridge from controller-centric to individual-controlled models
- **Demonstrates base standard extensibility**: Uses 27560:2025 structure for different control model

**Submission Strategy:**

Submit Co-Regulated Digital Privacy Profile (Type 2) as demonstration of base standard's flexibility to support transparency-by-default architectures beyond traditional data protection models. Appendix H clarifies relationship to other profile types without requiring their simultaneous standardization.

---

# Document Status

# Appendix J (Informative): AI System Context Implementation

**Status**: INFORMATIVE — This appendix does not affect conformance to the Universal Notice Receipt Profile. AI system transparency support is OPTIONAL for base profile conformance.

## J.1 AI System Notice Types

When `context_category="ai_system"`, the following `notice_type` values enable AI-specific transparency:

#### J.1.1 Automated Decision-Making Disclosure

- **notice_type**: "automated_decision_disclosure"
- **Use case**: Informing individuals that AI system will make or significantly influence decisions affecting them

- **Legal basis**: Convention 108+ Article 9 (automated decision rights), GDPR Article 22, ISO/IEC 42001 Annex B.8.2

**Example Notice Receipt**:

```
{
  "schema_version": "27560-UNIVERSAL-NOTICE-2025-1.0",
  "receipt_id": "ai-notice-001",
  "controller_identity_record_id": "CIR-CA-FINANCE-789",
  "notice_receipt_type": "ANCR Exchange Stage 1",
  "notice_type": "automated_decision_disclosure",
  "context_category": "ai_system",
  "ai_system_disclosure": {
    "system_name": "Credit Scoring Model v2.3",
    "intended_purpose": "Automated creditworthiness assessment",
    "decision_scope": "Loan approval up to $50,000 CAD",
    "human_oversight_available": true,
    "explainability_mechanism": "SHAP values provided on request via rights_access_point"
  },
  "scope_of_disclosure": "regional",
  "permissions_bundle": [
    "automated_decision_making",
    "human_review_on_request"
  ]
}
```

### J.1.2 AI Model Update Notification

- **notice_type**: "disclosure"
- **Use case**: Material change notification when AI model version changes significantly
- **Triggers**: Model retrained with new data, algorithm changed, performance metrics drift beyond threshold

**Example Material Change Disclosure**:

```
{
  "notice_type": "disclosure",
  "context_category": "ai_system",
  "material_change_description": "Credit scoring model updated from v2.3 to v3.0. New model trained on 2024 data; accuracy improved from 89% to 92%.",
  "change_effective_date": "2026-01-15",
  "impact_to_individual": "Previous credit scores may be recalculated under new model. Individuals may request manual review within 30 days.",
  "event_type": "ai_model_retrained"
}
```

#### J.1.3 AI System Deployment Notice

- **notice_type**: "notification"
- **Use case**: Initial notice when AI system begins processing individual data
- **Required for**: High-risk AI systems per EU AI Act Article 13, ISO/IEC 42001 Annex B.6.2.7

#### J.1.4 Performance Drift Disclosure

- **notice_type**: "disclosure"
- **Use case**: Material change when AI system performance degrades or exhibits unexpected behavior
- **Regulatory alignment**: ISO/IEC 42001 Annex B.6.2.6 monitoring requirements

---

### J.2 AI-Specific Authorization Types (ANCR Exchange Stage 2)

When individuals authorize AI system processing, `authorization_type` extends to include:

#### J.2.1 Automated Decision Consent

- **authorization_type**: "automated_decision_consent"
- **Legal basis**: Consent for automated decision-making per Convention 108+ Article 9
- **Required fields**:
  - `decision_scope`: What decisions AI will make
  - `human_review_availability`: How to request human oversight
  - `explainability_access`: Mechanism to obtain decision explanation

**Example Authorization**:

```
{
  "authorization_type": "automated_decision_consent",
  "consent_timestamp": "2025-12-12T10:00:00-05:00",
  "decision_scope": "Employment screening—resume filtering only; final hiring decision by human recruiter",
  "human_review_availability": "Request manual review within 14 days via rights_access_point",
  "explainability_access": "Decision factors provided automatically with rejection notice",
  "permissions_bundle": [
    "automated_resume_screening",
    "human_review_on_request",
    "explainability_report_generation"
  ],
  "withdrawal_mechanism": "Email privacy@example.com—withdrawal effective within 48 hours"
}
```

#### J.2.2 AI Training Data Consent

- **authorization_type**: "ai_training_data_consent"
- **Use case**: Specific consent for using individual's data to train or improve AI models
- **Distinct from**: Service delivery consent (processing for AI training is secondary purpose)

**Example**:

```
{
  "authorization_type": "ai_training_data_consent",
  "consent_timestamp": "2025-12-12T10:05:00-05:00",
  "training_purpose": "Improve recommendation algorithm accuracy",
  "data_retention_training": "Training data retained for model lifecycle; deleted when model decommissioned (estimated 24 months)",
  "opt_out_mechanism": "Disable via account settings—future interactions excluded from training",
  "anonymization_guarantee": "Personal identifiers removed before training; only behavioral patterns utilized"
}
```

### J.2.3 Explainability Request Authorization

- **authorization_type**: "explainability_request"
- **Use case**: Individual exercises right to explanation for automated decision
- **Regulatory basis**: GDPR Article 22(3), ISO/IEC 42001 Annex B.9.3 transparency objectives

## J.3 AI Notice Event Log Requirements

When `context_category="ai_system"`, the Notice Event Log SHALL record AI-specific events per ISO/IEC 42001 Annex B.6.2.8:

### J.3.1 Mandatory AI Events

| Notice Event Type | Trigger | ISO/IEC 42001 Reference | Logged Information |
|---|---|---|---|
| ai_decision_made | AI system makes or influences decision affecting individual | B.6.2.8 (event logs) | Decision ID, timestamp, outcome, confidence score, model version |
| ai_model_retrained | Model retrained or version updated | B.6.2.6 (operation monitoring) | Old version, new version, performance metrics, training data summary |
| human_override_exercised | Human reviewer overrides AI decision | B.9.3 (human oversight) | Override timestamp, reviewer ID, override reason, final outcome |
| explainability_requested | Individual requests decision explanation | B.8.2 (information for users) | Request timestamp, decision ID, explanation delivery method |

| Notice Event Type | Trigger | ISO/IEC 42001 Reference | Logged Information |
|---|---|---|---|
| ai_performance_drift_detected | Model performance below threshold or bias detected | B.6.2.6 (monitoring) | Metric name, expected value, actual value, detection timestamp |

### J.3.2 Event Log Query via Rights Access Point

Individuals MAY query AI-specific events via `rights_access_point`:

- "Show all automated decisions made about me in past 12 months"
- "Has my data been used for AI training?"
- "Were any AI decisions about me overridden by humans?"

**Example Event Log Entry**:

```
{
  "event_time": "2025-12-10T14:22:00-05:00",
  "event_type": "ai_decision_made",
  "entity_id": "CIR-CA-FINANCE-789",
  "decision_metadata": {
    "decision_id": "loan-app-12345",
    "model_version": "credit-scoring-v2.3",
    "outcome": "approved",
    "confidence_score": 0.87,
    "primary_factors": ["income_stability", "credit_history_length", "debt_to_income_ratio"]
  },
  "human_review_available": true
}
```

## J.4 High-Risk AI Enhanced Transparency

When AI system classified as **high-risk** per applicable framework (EU AI Act Annex III, ISO/IEC 42001 risk assessment), controllers SHALL enhance CIR with:

### J.4.1 AI System Documentation in CIR

Extend Controller Identification Record with `ai_system_documentation` object:

```
{
  "controller_identity_record_id": "CIR-EU-HR-AI-456",
  "ai_system_documentation": {
    "system_name": "Automated Resume Screening System",
    "risk_classification": "high_risk_per_eu_ai_act_annex_iii_4a",
    "conformity_assessment_body": "TÜV SÜD notified body #1234",
    "ce_marking_reference": "CE-AI-2025-567",
    "intended_purpose": "Pre-screen job applications for skills match; final hiring decision by human recruiter",
    "prohibited_use_cases": [
      "Sole determinant of hiring decision",
      "Personality assessment",
      "Discriminatory filtering"
    ],
    "human_oversight": {
      "oversight_type": "human_in_command",
      "override_available": true,
      "override_mechanism": "Hiring manager reviews all AI recommendations before decision",
      "oversight_competence_requirements": "Trained on bias detection and model limitations"
    },
    "performance_metrics": {
      "accuracy": 0.89,
      "fairness_audit_date": "2025-11-15",
      "demographic_parity_deviation": 0.04,
      "false_positive_rate": 0.08
    },
    "model_transparency": {
      "algorithm_type": "gradient_boosted_decision_trees",
      "explainability_method": "SHAP (SHapley Additive exPlanations)",
      "training_data_sources": "Anonymized historical hiring data 2020-2024; public job description corpus",
      "bias_mitigation_measures": [
        "Protected attributes excluded from training",
        "Fairness constraints applied during optimization",
        "Regular bias audits per ISO/IEC TR 24027"
      ]
    },
    "update_frequency": "quarterly_retraining_with_fairness_audit"
  }
}
```

### J.4.2 EU AI Act Article 13 Transparency Requirements

High-risk AI systems under EU AI Act SHALL disclose via notice receipt:

- AI system provider identity and contact (mapped to CIR fields)
- Intended purpose and limitations (ai_system_documentation.intended_purpose)
- Level of accuracy and known limitations (performance_metrics)
- Human oversight arrangements (human_oversight object)
- Instructions for use (available via rights_access_point)

### J.4.3 Conformity Assessment Documentation

For AI systems requiring conformity assessment (EU AI Act Article 43), CIR SHALL reference:

- Notified body identifier
- CE marking reference
- Technical documentation availability for supervisory authorities

**Notice Receipt Integration**:

```
{
  "context_category": "ai_system",
  "scope_of_disclosure": "international",
  "ai_risk_classification": {
    "framework": "eu_ai_act",
    "risk_level": "high_risk_annex_iii_4a_employment",
    "conformity_status": "ce_marked",
    "assessment_body": "TÜV SÜD #1234",
    "last_audit_date": "2025-10-20"
  }
}
```

---

## J.5 Cross-Border AI Model Deployment

When AI system training, deployment, or inference occurs across jurisdictions, enhanced transparency required:

### J.5.1 Training vs. Inference Jurisdiction Disclosure

Extend `recipient_jurisdictions` with AI-specific context:

```
{
  "scope_of_disclosure": "international",
  "recipient_jurisdictions": [
    {
      "country_code": "US",
      "role": "ai_model_training",
      "adequacy_status": "no_decision",
      "data_processed": "Training dataset—anonymized user interactions 2020-2024",
      "legal_regime": "FISA Section 702 permits government access to training data stored by US cloud providers"
    },
    {
      "country_code": "CA",
      "role": "ai_inference",
      "adequacy_status": "adequate",
      "data_processed": "Real-time inference—individual queries processed in Canadian data centers"
    }
  ]
}
```

### J.5.2 AI-Specific Surveillance Risks

Extend `surveillance_risks` to address AI model access:

```
{
  "surveillance_risks": {
    "disclosed": true,
    "jurisdictions": {
      "US": "AI model training data stored in US cloud subject to FISA Section 702 access. Government may access training datasets containing anonymized behavioral patterns.",
      "CN": "AI inference processing in China subject to National Intelligence Law Article 7 cooperation requirements. Inference logs may be subject to government access without notification."
    },
    "ai_specific_risks": [
      "Model parameters may reveal training data characteristics if subject to government access",
      "Inference logs document decision patterns and could be compelled for national security purposes",
      "Federated learning architecture limits but does not eliminate data transfer risks"
    ],
    "mitigation_measures": [
      "Differential privacy applied to training data (epsilon=1.0)",
      "Model parameters encrypted at rest using AES-256",
      "Inference logs retained for 30 days only; anonymized after",
      "Regular privacy impact assessments per ISO/IEC 42001 Section 6.1.4"
    ],
    "legal_frameworks": [
      "FISA Section 702 (USA—training data access)",
      "National Intelligence Law Article 7 (China—inference log access)",
      "EU AI Act Article 10 (data governance for high-risk AI)"
    ]
  }
}
```

### J.5.3 Model Parameter Transfer Transparency

For AI models trained in one jurisdiction and deployed in another:

```
{
  "transfer_mechanism": "legitimate_interest",
  "model_deployment_disclosure": {
    "training_jurisdiction": "US",
    "training_completion_date": "2025-09-30",
    "deployment_jurisdictions": ["CA", "GB", "AU"],
    "model_transfer_safeguards": [
      "Model weights do not contain raw personal data",
      "Differential privacy guarantees prevent training data reconstruction",
      "Model audited for fairness across deployment jurisdictions"
    ],
    "cross_jurisdiction_performance": {
      "CA": {"accuracy": 0.89, "fairness_audit": "2025-11-01"},
      "GB": {"accuracy": 0.87, "fairness_audit": "2025-11-05"},
      "AU": {"accuracy": 0.88, "fairness_audit": "2025-11-10"}
    }
  }
}
```

### J.5.4 Federated Learning Disclosure

For AI systems using federated learning or distributed training:

```
{
  "ai_training_architecture": "federated_learning",
  "federated_learning_disclosure": {
    "description": "Model trained across multiple jurisdictions without centralizing raw data",
    "participant_jurisdictions": ["CA", "US", "GB"],
    "data_transfer_minimal": true,
    "gradient_transfer_only": "Only model parameter updates exchanged; raw data remains in origin jurisdiction",
    "privacy_guarantees": [
      "Secure aggregation prevents individual contribution inference",
      "Differential privacy applied to gradient updates (epsilon=0.5)",
      "No raw personal data leaves origin jurisdiction"
    ]
  }
}
```

## J.6 Conformance and Standards Alignment

### J.6.1 Optional AI System Transparency Conformance

Organizations claiming **"AI System Transparency Extension"** conformance SHALL:

1. Implement Universal Notice Receipt Profile (mandatory base)
2. Use `context_category="ai_system"` when AI systems process personal data
3. Log AI-specific events per J.3 (ai_decision_made, ai_model_retrained, human_override_exercised)
4. Provide human oversight mechanism disclosure in `permissions_bundle` for automated decisions

5. Disclose AI model deployment jurisdictions when scope_of_disclosure="international"

### J.6.2 High-Risk AI Enhanced Conformance (Optional)

Organizations with high-risk AI systems MAY claim enhanced conformance by:

1. Publishing AI system documentation in CIR per J.4.1
2. Providing conformity assessment references (EU AI Act, ISO/IEC 42001 audits)
3. Enabling explainability requests via rights_access_point
4. Maintaining AI-specific Notice Event Log queryable by individuals

### J.6.3 ISO/IEC 42001 Integration

This profile implements ISO/IEC 42001 transparency requirements:

- **Annex B.6.2.7 (Technical Documentation)**: Mapped to `ai_system_documentation` in CIR
- **Annex B.6.2.8 (Event Logs)**: Mapped to AI-specific `event_type` values in Notice Event Log
- **Annex B.8.2 (Information for Users)**: Implemented via ANCR Exchange Stage 1 (Notice Receipt) with ai_system context
- **Annex B.9.3 (Human Oversight)**: Disclosed through `human_oversight` object and `permissions_bundle`

### J.6.4 ISO/IEC 27091 (AI Privacy) Coordination

ISO/IEC 27091 defines AI-specific privacy requirements; this profile provides the **bilateral receipt exchange mechanism** for 27091 transparency obligations.

**Division of responsibility**:

- **ISO/IEC 27091**: Defines what AI privacy obligations exist (data quality, fairness, transparency)
- **Universal Notice Receipt Profile J**: Defines how to transparently communicate AI obligations via notice receipts

**Cross-reference**: Organizations implementing ISO/IEC 27091 SHOULD use this profile's AI System Transparency Extension (Appendix J) for notice receipt generation and Notice Event Log maintenance.

## J.7 Implementation Guidance

**For Controllers Deploying AI Systems**:

1. Classify AI system risk level using applicable framework (EU AI Act, ISO/IEC 42001, jurisdictional regulations)
2. Extend CIR with `ai_system_documentation` if high-risk
3. Generate ANCR Exchange Stage 1 (Notice Receipt) with `context_category="ai_system"` before processing begins
4. Configure Notice Event Log to capture AI-specific events (J.3)
5. Provide explainability mechanism via `rights_access_point` for automated decisions

6. Update notice receipts when AI model version changes materially

**For Individuals Interacting with AI Systems**:

1. Review `ai_system_documentation` in CIR to understand AI decision scope
2. Verify `human_oversight_available` flag before authorizing automated decisions
3. Query Notice Event Log via `rights_access_point` to view AI decisions made about you
4. Exercise explainability request if automated decision outcome unclear
5. Request human review if AI decision appears erroneous or unfair

**For Regulators Overseeing AI Systems**:

1. Verify `ai_risk_classification` in CIR against applicable framework
2. Audit Notice Event Log for required AI events (ai_decision_made, human_override_exercised)
3. Validate conformity assessment references for high-risk AI systems
4. Check cross-border AI deployment transparency (training vs. inference jurisdictions)
5. Use public CIR registries to scale AI system transparency verification

---

**Appendix J Status**: INFORMATIVE — Deferred to v1.1 for normative specification

**Conformance Impact**: None—AI system transparency is OPTIONAL for Universal Notice Receipt Profile v1.0 base conformance

**V1.1 Scope**: AI-specific transparency will be standardized in future revision with:

- Normative AI  notice event log requirements coordinated with ISO/IEC 42001 Annex B.6.2.8
- High-risk AI enhanced transparency protocols aligned with EU AI Act implementation
- Cross-border AI model deployment transparency standards (training vs. inference jurisdiction disclosure)
- ISO/IEC 27091 coordination for AI privacy bilateral receipt exchange mechanisms

**Rationale**: AI governance infrastructure (automated decision disclosure, model retraining transparency, explainability mechanisms) extends beyond v1.0's core co-regulated transparency architecture. V1.0 demonstrates extensibility; v1.1 addresses operational AI transparency requirements after base infrastructure adoption.

---

## Document Status

---

## Appendix I (Informative): Consent Token Implementation Guidance

**Status**: INFORMATIVE — This appendix does not affect conformance to the Universal Notice Receipt Profile. Consent token support is OPTIONAL for base profile conformance.

## I.1 Consent Token Architecture

**Relationship to Notice Receipt**:

- Consent token is cryptographically bound to notice receipt identifier
- Token inherits permissions_bundle from ANCR Exchange Stage 2 (Consent Notice Receipt)
- Token enables consent portability without re-sharing raw receipt data

**Token Lifecycle**:

1. **Issuance**: Generated when individual authorizes ANCR Exchange Stage 2 receipt with principal_anchor
2. **Verification**: Controller validates token against CIR-ID and Notice Event Log
3. **Revocation**: Token invalidated through Notice Event Log state change
4. **Expiration**: Token validity tied to authorization validity_duration

**Cryptographic Binding**:

- Token includes HMAC or digital signature over: CIR-ID, receipt_id, permissions_bundle, authorization_timestamp
- Controller public key or shared secret enables third-party controller verification
- Token format: JWT (JSON Web Token), CBOR, or JSON-LD structured token standard

## I.2 Use Cases

**Agent-to-Agent Data Sharing with Directed Authorization**:

- Individual authorizes AI agent to share specific data with third-party controller
- Agent presents consent token proving authorization for secondary purpose
- Third-party controller verifies token against originating controller's CIR registry entry

**Cross-Controller Consented Authorization Portability**:

- Individual moves between service providers with consent token
- New controller verifies authorization scope from original controller's CIR-ID
- Enables data portability rights exercise without manual re-authorization
- Establishes foundation for international consent based international data transfers with secured governance policy integrity.

**Automated Rights Exercise**:

- Consent token encodes right-to-erasure or access request
- Controller processes request automatically upon token verification
- Notice Event Log updated with automated rights exercise event

**Break-the-Glass Audit Trail**:

- Emergency access generates special-purpose consent token
- Token logged with regulatory authority identifier
- Individual notified post-facto through Notice Event Log

## I.3 Technical Pattern

**Token Claims Structure** (maps to Universal Notice Receipt Profile fields):

```
{
  "iss": "controller_identity_record_id",
  "sub": "pii_principal_id",
  "aud": "recipient_controller_id",
  "exp": "expiration_timestamp",
  "iat": "issuance_timestamp",
  "jti": "receipt_id",
  "authorization": {
    "type": "consent_granted",
    "permissions_bundle": ["read", "process"],
    "purpose": "secondary_purpose_description",
    "scope_of_disclosure": "regional",
    "pii_categories": ["email", "name"],
    "retention_period": "P30D"
  },
  "principal_anchor": "did:example:123",
  "notice_event_log_id": "optional_log_reference"
}
```

**Verification Protocol**:

1. Recipient controller extracts `iss` (CIR-ID) from token
2. Lookup CIR-ID in public controller registry to obtain public key or verification endpoint
3. Validate token signature against controller's public key
4. Check token expiration and authorization scope applicability
5. Optional: Query Notice Event Log for revocation status

**Authorization Scope Encoding**:

- `permissions_bundle` array maps to ANCR Exchange Stage 2 (Consent Notice Receipt)
- `purpose` must match or be subset of original notice receipt purpose
- `scope_of_disclosure` constrains geographic or categorical sharing limits
- Token verification MUST fail if requested action exceeds encoded scope

**Revocation Mechanism**:

- Individual withdraws authorization → controller updates Notice Event Log with state change

- Revoked `receipt_id` added to revocation list (controller maintains)
- Token verification checks revocation list before accepting token
- Real-time revocation: controller provides revocation check API endpoint

## I.4 Security Considerations

**Token Bearer vs. Proof-of-Possession Models**:

- **Bearer**: Token holder can exercise authorization (suitable for trusted agent scenarios)
- **Proof-of-Possession**: Token must be accompanied by cryptographic proof of individual control (higher assurance)
- Recommendation: Use proof-of-possession for high-risk PII categories per scope of disclosure

**Replay Attack Prevention**:

- Include `jti` (receipt_id) as unique token identifier
- Controllers maintain used-token registry for single-use tokens
- Time-bound tokens with short `exp` for ephemeral authorization grants
- Nonce-based challenge-response for proof-of-possession flows

**Authorization Freshness Validation**:

- Token `iat` (issuance) must be after most recent material state change in Notice Event Log
- Controllers reject tokens issued before policy updates or material changes
- Individual must re-issue token after controller sends material change notification

**Privacy-Preserving Verification** (OPTIONAL):

- Zero-knowledge proof (ZKP) techniques enable verification without revealing full token claims
- Selective disclosure: Individual proves authorization scope without exposing other permissions
- Use case: Prove "age > 18" authorization without revealing exact birthdate
- Standards consideration: Align with W3C Verifiable Credentials for ZKP patterns

## I.5 Implementation Guidance

**For Controllers**:

1. Extend Notice Event Log to track token issuance and verification events
2. Implement token signing using controller identity key pair
3. Publish token verification endpoint or public key in CIR registry entry
4. Maintain revocation list synchronized with Notice Event Log state changes

**For Individuals**:

1. Store ANCR Exchange Stage 2 authorization receipts in personal data store or consent capable digital wallet
2. Generate consent tokens from stored receipts for secondary purpose sharing
3. Monitor Notice Event Log for controller material changes requiring token refresh
4. Revoke tokens by updating authorization state with originating controller

**For Third-Party Verifiers**:

1. Implement token verification against public controller registry
2. Respect scope_of_disclosure constraints in token claims
3. Log token verification events for audit trail
4. Reject tokens from controllers not in trusted registry

## I.6 Standards Alignment

**Related Standards**:

- **W3C Decentralized Identifiers (DIDs)**: CIR-ID and principal_anchor may be expressed as DIDs
- **W3C Verifiable Credentials (VCs)**: Consent tokens may be implemented as VCs
- **OAuth 2.0 / UMA 2.0**: Token patterns align with resource authorization flows
- **ISO/IEC 27091 (Gen AI)**: Consent tokens address AI agent authorization requirements

**Interoperability Commitment**:

- Token format should support multiple serializations (JWT, CBOR, JSON-LD)
- Verification protocol should be transport-agnostic (HTTP, DIDComm, etc.)
- Authorization semantics mapped to W3C Data Privacy Vocabulary (DPV) for machine-readability

## I.7 Conformance Considerations

- Non-token implementations remain fully conformant to Universal Notice Receipt Profile

**High-Assurance Implementations**:

Consent token support is RECOMMENDED for:

- Multi-controller data sharing scenarios
- Agentic AI authorization delegation
- Cross-jurisdictional authorization portability
- Regulatory enforcement automation contexts

## I.8 Future Development

This consent token pattern enables:

- Consent wallet applications holding tokens for agentic AI data sharing

- Trustmark validation of token-capable controllers
- Digital governance using consent tokens as authorization proof
- Agentic AI with consent tokens for automated permission negotiation

---

**Appendix I Status**: INFORMATIVE — Deferred to v1.1 for normative specification

**Conformance Impact**: None—Consent token support is OPTIONAL for Universal Notice Receipt Profile v1.0 base conformance

**V1.1 Scope**: Consent token infrastructure will be standardized in future revision with:

- Normative cryptographic binding requirements (JWT, CBOR, JSON-LD formats)
- Token verification protocol specifications for third-party controllers
- Revocation mechanism standards synchronized with Notice Event Log
- W3C Verifiable Credentials and DID alignment for interoperability
- Zero-knowledge proof patterns for privacy-preserving verification

**Rationale**: Portable authorization tokens (ANCR Exchange Stage 4) address cross-controller consent portability, agentic AI coordination, and SSI/DID infrastructure—advanced scenarios beyond v1.0's bilateral receipt generation focus. V1.0 establishes transparency-by-default architecture; v1.1 addresses authorization portability after base infrastructure proves viable.

---

# Appendix H: Derivative Digital Transparency Controls Under Convention 108+ Proportionality and Reciprocity Principles

**Subtitle**: Operationalizing Data Protection Rights for Digital Identification Technologies

## H.1 Executive Summary

Convention 108+ Articles 8 (transparency), 9 (proportionality), 12 (mutual assistance), and 14 (cross-border flows) mandate **proportionate and reciprocal transparency rights** when digital identification technologies are deployed. Current data protection frameworks (DPV/GDPR) were designed for analog contexts where notice, identification, and physical observation of privacy risks were inherent to face-to-face consent interactions.

**The Gap**: Digital identification enables real-time global surveillance, cross-border data flows, and persistent tracking—creating new categories of risk that analog-era rights frameworks fail to address.

**The Solution**: This appendix documents **eight derivative digital transparency controls** required by Convention 108+ treaty obligations when controllers deploy digital identification technologies. These are not new rights—they are **proportionate extensions** of existing data protection rights updated for digital contexts.

**v1.0 Profile Implementation**: ISO/IEC 27560:2025 Universal Notice Receipt Profile operationalizes these eight derivative controls through specific fields and mechanisms, providing the first enforceable implementation of Convention 108+ digital transparency requirements.

---

## H.2 Legal Foundation: Convention 108+ Mandates Proportionate Digital Transparency

**Article 8 (Transparency Obligations)**:

> "Each Party shall provide that the controller informs the data subjects of: his or her identity and habitual residence or establishment; the legal basis and the purposes of the intended processing..."[1]

**Digital Context Requirement**: If controllers can digitally identify individuals **before collection** (cookies, device fingerprinting, metadata capture), individuals need controller identity **before inference**.

**Article 9 (Proportionality Principle)**:

> "Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned..."[1]

**Digital Context Requirement**: Risk increases with **scope of disclosure** (local → international). Transparency obligations must be **proportionate to digital privacy risk**.

**Article 12 (Mutual Assistance)**:

> "The Parties shall afford one another mutual assistance in enforcing this Convention..."[1]

**Digital Context Requirement**: Cross-border enforcement requires **bilateral proof mechanisms** that enable regulatory cooperation without identifying data subjects.

**Article 14 (Transborder Flows)**:

> "When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to this Convention, the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convention is secured."[1]

**Digital Context Requirement**: Informed consent for cross-border transfers requires disclosure of **jurisdiction-specific surveillance risks** and **derogations to data subject rights**.

**Article 11.3 (Derogations Transparency)**:

> "In addition to the exceptions allowed for in paragraph 1 of this article, with reference to processing activities for national security and defense purposes, each Party may provide, by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim, exceptions to Article 4 paragraph 3, Article 14 paragraphs 5 and 6 and Article 15, paragraph 2..."[1]

**Digital Context Requirement**: If national security laws **derogate** Convention 108+ Article 9 rights (access, rectification, erasure), individuals must be informed **which rights are suspended** before consent.

---

## H.3 Eight Derivative Digital Transparency Controls

Each derivative control includes:

1. **Existing Right** (data protection foundation)
2. **Why Derivative is Required** (digital identification creates new risk)
3. **Convention 108+ Mandate** (treaty obligation)
4. **v1.0 Operationalization** (specific profile field/mechanism)
5. **Proportionality Rationale** (why this scales to risk)
6. **Reciprocity Mechanism** (bilateral proof enabling enforcement)

---

### H.3.1 Controller-ID Before Inference

**Derivative of**: GDPR Article 13/14 (right to be informed of controller identity)

**Existing Right**: Individual has right to know controller identity at time of data collection.

**Why Derivative is Required**:

- Original assumes identification happens **at collection** (face-to-face, paper forms)
- Digital identification happens **before collection** (cookies set on page load, device fingerprinting, IP logging)
- **Proportionate update**: Controller must identify **before inferring identifier**, not after

**Convention 108+ Mandate**:

- Article 8 (transparency): Controller identity must be provided
- Article 9 (proportionality): If controller can infer identity instantly, individual needs controller identity instantly

**v1.0 Operationalization**:

- Section 5.3: Controller Identification Record (CIR) published **before** any processing
- Section 5.4.1: CIR accessible at `/.well-known/transparency` (public, no authentication required)
- Section 6.1: `controller_identity_record_id` field in ANCR Exchange Stage 1 (Notice Receipt)
- ANCR Exchange Stage 1 generated **before** `pii_principal_id` collected (anonymous-by-default)

**Proportionality Rationale**:

- Digital identification is instantaneous and global—controller accountability must precede inference
- Analog contexts had inherent controller visibility (physical presence)—digital contexts require explicit CIR publication

**Reciprocity Mechanism**:

- Public CIR registries enable **mutual assistance** (Article 12) without identifying data subjects
- Regulatory authorities verify controller identity through registry lookup, not by accessing individual identifiers

**Matrix Entry**:

| Right | DPV/GDPR | v1.0 | Convention 108+ Mandate | Gap |
|---|---|---|---|---|
| **Controller-ID Before Inference** | ⚠️ Partial (Article 13—info "at time of collection") | ✅ Section 5.3 CIR + Stage 1 | Article 8 + 9 | No mechanism to provide controller ID **before** digital inference begins |

## H.3.2 Scope of Disclosure Transparency

**Derivative of**: GDPR Article 13.1(c) (purposes of processing)

**Existing Right**: Individual has right to know processing purposes.

**Why Derivative is Required**:

- Original assumes **single jurisdiction** or explicit transfer notice
- Digital identification enables **instant global disclosure** (local → international in milliseconds via real-time bidding, cloud sync)
- **Proportionate update**: Individual needs **geographic/categorical scope** as risk metric

**Convention 108+ Mandate**:

- Article 9 (proportionality): Risk increases with scope; transparency must match
- Article 14 (cross-border transfers): Additional safeguards required when data crosses borders

**v1.0 Operationalization**:

- Section 3.6: `scope_of_disclosure` definition (child, youth, vulnerable, community, regional, national, international)
- Section 5.4.1: Risk-proportionate field requirements based on scope
- Section 6.1.2.1: `scope_of_disclosure` field (enum)
- Section 7.1 #9: Scope escalation requires new consent permission

**Proportionality Rationale**:

- Local processing (device-only) = minimal risk → minimal transparency
- International disclosure (cross-border) = high risk → enhanced transparency (surveillance risks, jurisdiction disclosure)

**Reciprocity Mechanism**:

- Notice Event Log tracks scope changes with timestamps
- Material scope escalation triggers notification requirement
- Bilateral receipts prove individual was informed of scope **before** authorization

**Matrix Entry**:

| Right | DPV/GDPR | v1.0 | Convention 108+ Mandate | Gap |
|---|---|---|---|---|
| **Scope of Disclosure Transparency** | ❌ Missing (purpose != scope) | ✅ Section 3.6, 5.4.1, 6.1.2.1 | Article 9 + 14 | No concept of geographic/categorical scope as risk metric; treats "lawful processing" as binary |

### H.3.3 Digital Surveillance Risk Disclosure

**Derivative of**: GDPR Article 46 (appropriate safeguards for transfers)

**Existing Right**: Individual has right to know transfer safeguards.

**Why Derivative is Required**:

- Original lists "adequacy" as sufficient
- Digital identification in FISA 702 jurisdictions enables **government surveillance without notification**
- **Proportionate update**: Individual needs **explicit surveillance law disclosure** (FISA 702, IPA 2016, National Intelligence Law) before consent

**Convention 108+ Mandate**:

- Article 14.2 (transfers): Transfers require individual notification of risks
- ECHR Article 8: Proportionate interference with privacy requires transparency
- Article 11.3 (derogations): National security exceptions must be necessary and proportionate

**v1.0 Operationalization**:

- Section 6.1.2.3: `surveillance_risks` object with `disclosed` boolean + jurisdiction descriptions
- Section 6.1.2.3: `legal_frameworks` array (e.g., "FISA Section 702", "IPA 2016 Part 6")
- Section 6.1.2.3: `mitigation_measures` array documenting safeguards
- Section 6.1.2.4: `surveillance_disclosed_at_consent` boolean proving informed consent

**Proportionality Rationale**:

- Schrems II invalidated Privacy Shield because surveillance risks were **not disclosed** before consent
- Proportionate transparency: if government can access data without notification, individual must know **before** consenting to transfer

**Reciprocity Mechanism**:

- `transfer_consent_validation` object provides bilateral proof of surveillance disclosure
- Notice Event Log records `surveillance_disclosed_at_consent` timestamp
- Regulators verify informed consent through receipt validation

**Matrix Entry**:

| Right | DPV/GDPR | v1.0 | Convention 108+ Mandate | Gap |
|---|---|---|---|---|
| **Digital Surveillance Risk Disclosure** | ❌ Missing (Article 46 safeguards vague) | ✅ Section 6.1.2.3 `surveillance_risks` | Article 14.2 + ECHR Article 8 + Article 11.3 | No requirement to disclose **specific surveillance laws** (FISA 702, IPA 2016); adequacy deemed sufficient |

## H.3.4 Bilateral Notice Proof (Two-Factor Notice)

**Derivative of**: GDPR Article 7.1 (controller must demonstrate consent)

**Existing Right**: Controller must prove consent was obtained.

**Why Derivative is Required**:

- Original assumes **controller holds unilateral record**
- Digital identification enables **automated processing without human verification**
- **Reciprocal update**: Both parties must hold **cryptographically verifiable proof** (2FN)

**Convention 108+ Mandate**:

- Article 8 (transparency): Notice must be provided in "intelligible form"
- Article 12 (mutual assistance): Enforcement requires bilateral verification mechanisms

**v1.0 Operationalization**:

- Section 5.5: Two-Factor Notice (2FN) pattern specification
- Section 5.4.1: CIR registrar blind data notary signatures
- Section 6.1: `two_factor_notice_indicator` boolean field
- Stage 1 + Stage 2: Both parties hold synchronized receipt copies

**Proportionality Rationale**:

- Unilateral controller records enable "he said, she said" disputes
- Bilateral receipts provide **non-repudiation**: controller cannot claim individual was not notified

**Reciprocity Mechanism**:

- Individual holds receipt independently—can prove notice without controller cooperation
- Regulators validate receipts against CIR registry signatures
- Third-party verification through public CIR registries

**Matrix Entry**:

| Right | DPV/GDPR | v1.0 | Convention 108+ Mandate | Gap |
|---|---|---|---|---|
| **Bilateral Notice Proof (2FN)** | ⚠️ Partial (Article 7.1 controller proof only) | ✅ Section 5.5 2FN + registrar signatures | Article 8 + 12 | Individual has no independent proof; must rely on controller records |

### H.3.5 Notice Event Log Access

**Derivative of**: GDPR Article 15 (right to access personal data)

**Existing Right**: Individual has right to access personal data held by controller.

**Why Derivative is Required**:

- Original assumes **static dataset** held by controller
- Digital identification generates **continuous processing events** (each pageview = new inference, each disclosure = new event)
- **Proportionate update**: Individual needs access to **append-only audit trail** of all transparency state changes

**Convention 108+ Mandate**:

- Article 8 (transparency): Information in "intelligible form"
- Article 9 (proportionality): Continuous processing requires continuous transparency
- EU Regulation 2018/1725 Article 88: Operational personal data logging requirements

**v1.0 Operationalization**:

- Section 5.6: Notice Event Log specification (append-only structure)
- Section 6.2: `notice_event_log_url` field (queryable endpoint)
- Section 5.6: Event types (notice_issued, consent_granted, material_change, rights_exercised)
- Appendix C: Rights access via CIR `rights_access_point`

**Proportionality Rationale**:

- Static privacy policies inadequate for dynamic digital processing
- Continuous event logging proportionate to continuous digital identification

**Reciprocity Mechanism**:

- Notice Event Log accessible via CIR `rights_access_point` (no authentication required for transparency state queries)
- Both parties can verify log integrity through cryptographic hashing
- Regulators audit logs without controller gatekeeping

**Matrix Entry**:

| Right | DPV/GDPR | v1.0 | Convention 108+ Mandate | Gap |
|---|---|---|---|---|
| **Notice Event Log Access** | ⚠️ Partial (Article 15 static access) | ✅ Section 5.6 + 6.2 `notice_event_log_url` | Article 8 + 9 + EU 2018/1725 Art. 88 | No mechanism for continuous audit trail; manual access requests inadequate for real-time processing |

## H.3.6 Autonomous Consent Withdrawal

**Derivative of**: GDPR Article 7.3 (right to withdraw consent)

**Existing Right**: Individual has right to withdraw consent as easily as giving it.

**Why Derivative is Required**:

- Original assumes **manual request to controller** (30-day response time)
- Digital identification processes data **in real-time** across distributed systems
- **Reciprocal update**: If processing is automated, withdrawal must be **automated and immediate**

**Convention 108+ Mandate**:

- Article 9 (proportionality): Withdrawal mechanism must match processing speed
- Article 8 (transparency): Withdrawal status must be transparent in real-time

**v1.0 Operationalization**:

- Section 7.1 #9: Material change triggers automatic consent invalidation
- Section 15: ANCR Exchange Stage 4 (Consent Token) with `portability_scope` validation
- Notice Event Log: Withdrawal recorded with timestamp; controllers query log to check authorization status

**Proportionality Rationale**:

- Real-time processing requires real-time withdrawal capability
- 30-day response inadequate when data processed milliseconds after collection

**Reciprocity Mechanism**:

- Individual updates Notice Event Log independently (no controller permission required for withdrawal)
- Controllers query log to verify authorization remains valid
- Automated enforcement: systems check log before processing

**Matrix Entry**:

| Right | DPV/GDPR | v1.0 | Convention 108+ Mandate | Gap |
|---|---|---|---|---|
| **Autonomous Consent Withdrawal** | ⚠️ Partial (Article 7.3 requires controller cooperation) | ✅ Section 7.1 #9 + Stage 4 token validation | Article 9 | Manual withdrawal inadequate for automated processing; 30-day response delay violates proportionality |

### H.3.7 Active State Transparency

**Derivative of**: GDPR Article 12.1 (transparent information)

**Existing Right**: Individual has right to transparent information about processing.

**Why Derivative is Required**:

- Original assumes **static privacy policy**
- Digital identification enables **dynamic processing state** (active/inactive, scope changes in real-time)
- **Proportionate update**: Individual needs **real-time transparency signaling** (like SSL/TLS for privacy)

**Convention 108+ Mandate**:

- Article 8 (transparency): Information must be accessible and intelligible
- Article 9 (proportionality): High-risk contexts require active state monitoring

**v1.0 Operationalization**:

- Section 11: TATA Level 4 (Active State + Physical Verification)
- Section 17.2.1: Active State Synchronic Validation (CIR hash binding in tokens)
- Editorial notes: HABNI trustmark for active state signaling (v1.1)

**Proportionality Rationale**:

- Static policies inadequate for dynamic processing contexts
- Real-time signaling proportionate to real-time surveillance

**Reciprocity Mechanism**:

- Active state visible to individual without requesting access
- CIR hash validation prevents controllers from serving stale policies
- Automated detection of policy violations

**Matrix Entry**:

| Right | DPV/GDPR | v1.0 | Convention 108+ Mandate | Gap |
|---|---|---|---|---|
| **Active State Transparency** | ❌ Missing (Article 12.1 static transparency) | ✅ Section 11 TATA L4 + 17.2.1 synchronic validation | Article 8 + 9 | No concept of real-time transparency state; privacy policies updated without individual notification |

### H.3.8 Notice of Derogation to Digital Surveillance Rights

**Derivative of**: GDPR Article 13.2(b) (right to be informed of rights) + Article 21 (right to object)

**Existing Rights**:

- Right to be informed of data subject rights
- Right to object to processing
- Convention 108+ Article 9 (rights of access, rectification, erasure)

**Why Derivative is Required**:

- Original assumes rights are **universal and enforceable**
- Digital identification in derogation jurisdictions **suspends Article 9 rights** via national security exceptions
- **Proportionate update**: Individual must be informed **which rights are derogated and under what legal authority** before consent

**Convention 108+ Mandate**:

- Article 11.3: Derogations for national security must be "necessary and proportionate" and subject to "independent and effective review"
- Article 8 (transparency): Individuals must be informed of legal basis—derogation **is part of legal basis**
- Article 5.2 (informed consent): Consent must be "informed"—cannot be informed if rights derogations are hidden

**v1.0 Operationalization**:

**New Field Addition to Section 6.1.2.3 (Cross-Border Transfer Fields)**:

```
"digital_surveillance_risks": {
  "fisa_702_applies": true,
  "rights_derogations": [
    {
      "derogation_authority": "50 U.S.C. § 1881a (FISA 702)",
      "derogated_rights": [
        "right_to_access",
        "right_to_erasure",
        "right_to_be_informed_of_processing"
      ],
      "legal_basis_for_derogation": "national_security",
      "independent_oversight": "FISA Court (ex parte proceedings)",
      "derogation_disclosed_at_consent": true
    }
  ]
}
```

**Field Definitions**:

- **rights_derogations** (array): Convention 108+ Article 11 derogations affecting this transfer
- **derogation_authority** (string): Legal citation (e.g., FISA 702, IPA 2016 Part 6, National Intelligence Law Article 7)
- **derogated_rights** (array): Which Article 9 rights are suspended (access, rectification, erasure, objection, portability, notification)
- **legal_basis_for_derogation** (enum): national_security | defence | public_safety | prevention_of_crime
- **independent_oversight** (string): Article 11.3 "independent and effective review" mechanism description
- **derogation_disclosed_at_consent** (boolean): Proof individual was informed before consent

**Proportionality Rationale**:

- Article 11.3 requires derogations be "necessary and proportionate"—individual cannot assess proportionality if derogations are secret
- If government can suspend rights via legal authority, individual must know **which rights are suspended** to make informed decision
- Schrems II central issue: individuals consenting to US transfers were **not informed** that FISA 702 derogates their right to be notified of surveillance

**Reciprocity Mechanism**:

- `transfer_consent_validation` object proves individual was informed of derogations before consent
- Notice Event Log records `derogation_disclosed_at_consent` timestamp
- Regulators verify informed consent through receipt validation—adequacy determinations require derogation disclosure

**Matrix Entry**:

| Right | DPV/GDPR | v1.0 | Convention 108+ Mandate | Gap |
|---|---|---|---|---|
| **Notice of Derogation to Digital Surveillance Rights** | ❌ Missing (GDPR Article 23 permits restrictions without disclosure) | ✅ Section 6.1.2.3 `rights_derogations` | Article 11.3 + Article 8 + Article 5.2 | Individuals cannot assess proportionality if rights derogations are secret; Schrems II invalidated Privacy |

| Right | DPV/GDPR | v1.0 | Convention 108+ Mandate | Gap |
|---|---|---|---|---|
| | | | | Shield partially due to lack of derogation transparency |

**Legal Precedent**:

- CJEU *Schrems II* (C-311/18): Privacy Shield invalidated because US surveillance laws (FISA 702, EO 12333) **derogate EU data subject rights** without adequate transparency or oversight
- EDPB Recommendations 01/2020: Transfer Impact Assessments must evaluate **whether destination jurisdiction laws enable government access** that undermines Article 9 rights

## H.4 Cross-Border Transfer Rights: Schrems II Case Study

**The Gap**: GDPR Articles 44-50 require "appropriate safeguards" for cross-border transfers but provide no mechanism to disclose **jurisdiction-specific surveillance risks** or **rights derogations** before consent.

**Schrems II Holding**: Privacy Shield inadequate because:

1. FISA Section 702 permits US government surveillance of non-US persons **without notification**
2. EU data subjects have **no effective remedy** (FISA Court proceedings are ex parte)
3. This constitutes **derogation of GDPR Article 15 (access) and Article 79 (effective remedy)** without adequate safeguards

**Convention 108+ Article 14 Requirement**:

> "When the recipient is subject to the jurisdiction of a State... which is not Party to this Convention, the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convention is secured."

**v1.0 Solution**:

- Section 6.1.2.3 `surveillance_risks` field enables **explicit disclosure** of FISA 702 / IPA 2016 / National Intelligence Law
- Section 6.1.2.3 `rights_derogations` array documents **which Article 9 rights are suspended** in destination jurisdiction
- Section 6.1.2.4 `transfer_consent_validation.surveillance_disclosed_at_consent` proves individual was informed **before** consent

**Result**: v1.0 provides first **enforceable mechanism** for Convention 108+ Article 14 compliance—informed consent impossible without surveillance risk and derogation transparency.

## H.5 Enforcement Architecture: Proportionality Through Co-Regulated Infrastructure

**How Derivative Controls Enable Enforcement**:

**1. Controller-ID Before Inference** → CIR registries enable regulatory verification at scale

- Regulators query public registry to verify controller accountability
- No need to access individual identifiers—enforcement through transparency infrastructure

**2. Scope of Disclosure** → Risk-proportionate regulatory oversight

- Local/child scope = minimal oversight (self-assertion)
- International scope = enhanced oversight (registry verification + surveillance disclosure)

**3. Surveillance Risk Disclosure** → Adequacy determinations with enforceable standards

- Regulators require `surveillance_risks` field completion for cross-border transfers
- Automated adequacy checks: if destination jurisdiction = FISA 702, require disclosure or block transfer

**4. Bilateral Notice Proof (2FN)** → Article 12 mutual assistance

- Cross-border enforcement through receipt validation
- Regulators in Country A validate receipts from controllers in Country B using public CIR registries

**5. Notice Event Log** → Automated compliance verification

- Regulators query logs to verify transparency state changes
- Continuous oversight replaces periodic manual audits

**6. Autonomous Withdrawal** → Individual enforcement without regulator dependency

- Individual updates log; controllers automatically honor withdrawal
- Scales enforcement beyond regulatory capacity

**7. Active State Transparency** → Real-time violation detection

- Synchronic validation (Section 17.2.1) detects stale policies automatically
- Tokens invalid if CIR hash doesn't match registry—prevents circumvention

**8. Derogation Notice** → Informed consent verification

- Regulators verify `derogation_disclosed_at_consent` before approving adequacy
- Schrems II compliance through enforceable field requirement

## H.6 Summary Table: Derivative Digital Transparency Controls

| Control | Foundation Right | Convention 108+ Mandate | v1.0 Field/Mechanism | Critical Gap Addressed |
|---|---|---|---|---|
| **1. Controller-ID Before Inference** | GDPR Art. 13/14 (informed of controller) | Article 8 + 9 | Section 5.3 CIR, Stage 1 `controller_identity_record_id` | Timing inversion: accountability before inference |

| Control | Foundation Right | Convention 108+ Mandate | v1.0 Field/Mechanism | Critical Gap Addressed |
|---|---|---|---|---|
| **2. Scope of Disclosure** | GDPR Art. 13.1(c) (purposes) | Article 9 + 14 | Section 3.6, 6.1.2.1 `scope_of_disclosure` | No geographic/categorical risk metric |
| **3. Surveillance Risk Disclosure** | GDPR Art. 46 (transfer safeguards) | Article 14.2 + ECHR Art. 8 + Art. 11.3 | Section 6.1.2.3 `surveillance_risks` | No specific surveillance law disclosure (FISA 702, IPA 2016) |
| **4. Bilateral Notice Proof (2FN)** | GDPR Art. 7.1 (controller proof) | Article 8 + 12 | Section 5.5 2FN, registrar signatures | Unilateral controller records; no individual proof |
| **5. Notice Event Log Access** | GDPR Art. 15 (access) | Article 8 + 9 + EU 2018/1725 Art. 88 | Section 5.6, 6.2 `notice_event_log_url` | No continuous audit trail for real-time processing |
| **6. Autonomous Withdrawal** | GDPR Art. 7.3 (withdraw consent) | Article 9 | Section 7.1 #9, Stage 4 token validation | Manual withdrawal inadequate for automated processing |
| **7. Active State Transparency** | GDPR Art. 12.1 (transparent info) | Article 8 + 9 | Section 11 TATA L4, 17.2.1 synchronic validation | No real-time transparency state |
| **8. Derogation Notice** | GDPR Art. 13.2(b) + 21 (rights info) | Article 11.3 + 8 + 5.2 | Section 6.1.2.3 `rights_derogations` | Individuals cannot assess proportionality if derogations secret |

## H.7 Recommendations

**For Privacy Commissioners**:

1. Require these eight derivative controls in **adequacy determinations** for cross-border data transfers
2. Adopt CIR registry infrastructure for **regulatory capacity at scale**
3. Pilot v1.0 profile with volunteer controllers across Commonwealth jurisdictions
4. Use Notice Event Log verification for **automated compliance oversight**

**For Standards Bodies (ISO/IEC JTC 1/SC 27/WG 5)**:

1. Adopt v1.0 field mappings as **normative implementation** of Convention 108+ digital transparency
2. Reference this appendix in CD balloting materials
3. Coordinate with EDPB / supervisory authorities for regulatory alignment

**For Regulators**:

1. Integrate `surveillance_risks` and `rights_derogations` fields into **Transfer Impact Assessment** requirements
2. Mandate CIR publication for **controllers processing international transfers**

3. Enable individuals to **lodge complaints using notice receipt evidence**

## H.8 Conclusion

These eight derivative digital transparency controls are **not optional enhancements**—they are **treaty obligations** under Convention 108+ when controllers deploy digital identification technologies. Current data protection frameworks (DPV/GDPR) were designed for analog contexts and lack mechanisms to operationalize these requirements.

**ISO/IEC 27560:2025 Universal Notice Receipt Profile v1.0** provides the **first enforceable implementation** through:

- **Controller-ID first** architecture (Section 5.3-5.4)
- **Risk-proportionate transparency** through scope of disclosure (Section 3.6, 6.1.2.1)
- **Cross-border surveillance disclosure** (Section 6.1.2.3)
- **Bilateral proof mechanisms** enabling Article 12 mutual assistance (Section 5.5)
- **Notice Event Logs** for continuous transparency (Section 5.6)
- **Autonomous enforcement** through Stage 4 portable tokens (Section 15, 17.2.1)
- **Derogation transparency** for informed consent (Section 6.1.2.3 `rights_derogations`)

**This profile operationalizes Convention 108+ for the digital age**—enabling privacy-enabling data control (individual-centric) rather than privacy-preserving data protection (controller-centric).[2]

**Version**: 1.0 Final Submission Draft

**Historical Context**: This profile completes the Minimum Viable Consent Receipt (MVCR) specification originated by the Kantara Initiative, which was adopted as the foundation for ISO/IEC TS 27560:2023 and referenced in ISO/IEC 29184:2020 Appendix D. The universal notice receipt architecture implements Anchor Notice and Consent Receipt exchange, demonstrating the original MVCR purpose to replace terms and conditions with co-regulated (standard privacy policy) Convention 108+ as universal standard transparency infrastructure applicable to safety, security, data protection and digital privacy contexts.