# IETF Internet-Draft: Well-Known URI for Controller Transparency Records

**Document Type**: IETF Internet-Draft (Standards Track)

**Intended Status**: Proposed Standard

**Target**: RFC Publication

**Expires**: Six months from publication

## Abstract

This document registers the `/.well-known/transparency` URI suffix for publishing Controller Identification Records (CIRs) and privacy transparency information per ISO/IEC 27560:2025 and Council of Europe Convention 108+ requirements. This well-known location enables automated discovery of controller accountability information before data processing begins, supporting transparency-by-default architecture and co-regulated privacy infrastructure.

## Status of This Memo

## Copyright Notice

## Table of Contents

# 1. Introduction

## 1.1 Problem Statement

Current data protection frameworks require controllers to provide transparency information to individuals, yet lack a standardized location for publishing this information in a machine-readable format. This creates several problems:

- **Discovery Challenge**: Individuals and automated systems cannot reliably locate controller accountability information
- **Verification Gap**: No standard mechanism exists for verifying controller identification before data processing begins
- **Enforcement Friction**: Regulatory authorities face high costs auditing compliance across fragmented transparency mechanisms

- **Rights Exercise Barriers**: Individuals struggle to determine where and how to exercise data protection rights

## 1.2 Solution Overview

This document defines a well-known URI location for publishing Controller Identification Records (CIRs) and associated transparency information. By establishing `/.well-known/transparency` as the standard location, this specification enables:

- **Automated Discovery**: Systems can reliably locate controller transparency information
- **Anonymous-by-Default Architecture**: Controllers identify themselves before requesting individual identification
- **Independent Verification**: Third parties can generate notice receipts using publicly available controller information
- **Regulatory Scalability**: Automated verification through public registries

## 1.3 Use Cases

**Consent Receipt Generation**: Individuals or their agents retrieve CIR to generate notice receipts documenting transparency state before providing consent.

**Rights Exercise**: Individuals locate the rights access point to exercise Convention 108+ data subject rights (access, rectification, erasure, portability).

**Regulatory Enforcement**: Data protection authorities verify controller compliance through automated CIR validation against public registries.

**Cross-Border Transfers**: Controllers disclose recipient jurisdictions and transfer mechanisms, enabling informed consent for international data flows.

**Multi-Stakeholder Verification**: Researchers, civil society, and verification services independently assess controller transparency practices.

## 1.4 Relationship to Existing Standards

- **RFC 8615**: This specification uses the well-known URI framework for standardized resource discovery
- **ISO/IEC 27560:2025**: CIR structure aligns with PII processing record information structure

- **Convention 108+**: Transparency requirements operationalized through CIR publication
- **W3C Data Privacy Vocabulary**: Legal  semantic vocabulary and machine readable interoperability for privacy concepts

## 2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

**Controller**: Natural or legal person, public authority, agency, or other body which determines the purposes and means of processing personally identifiable information (PII). (Convention 108+ Article 2(d))

**Controller Identification Record (CIR)**: Structured grouping of publicly required controller information, enabling independent notice receipt generation and rights access.

**CIR-ID**: Unique public reference enabling registry verification and cross-jurisdictional lookup of controller identification.

**Notice Receipt**: Bilateral record documenting controller notification for PII processing under any legal basis, held by both controller and individual.

**Two-Factor Notice (2FN)**: Pattern where controller presents notice AND generates proof-of-notice record held by both parties.

**Rights Access Point**: URI or contact information enabling individuals to exercise Convention 108+ data subject rights.

**Scope of Disclosure**: Risk categorization determining proportionate transparency obligations (child, youth, vulnerable, community, regional, national, international).

## 3. Well-Known URI Registration

### 3.1 Registration Template

Per RFC 8615 Section 5, this document requests registration of the following well-known URI:

**URI suffix**: `transparency`

**Change controller**: IETF

**Specification document**: [this RFC]

**Related information**:

- ISO/IEC 27560:2025 (PII Processing Record Information Structure)
- Council of Europe Convention 108+ (Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data)
- ISO/IEC 29100:2011 (Privacy framework)

**Status**: permanent

### 3.2 URI Construction

Controllers SHALL publish their Controller Identification Record at:

```
https://<authority>/.well-known/transparency
```

Or with explicit file reference:

```
https://<authority>/.well-known/transparency/notice.txt
```

Both formats are semantically equivalent. Systems SHOULD check both locations, with `/.well-known/transparency` taking precedence.

### 3.3 Alternative Locations

For controllers without TLS certificates or specialized deployments, alternative publication locations MAY include:

- Root-level: `https://<authority>/notice.txt`
- Custom path with redirect: Any controller-specified location that redirects to the CIR

However, `/.well-known/transparency` is the RECOMMENDED standard location for automated discovery.

## 4. Controller Transparency Record Format

### 4.1 Media Type

CIR documents MUST be served with Content-Type `application/json` or `application/ld+json` for JSON-LD formatted records.

## 4.2 Required Fields

A conformant CIR MUST include:

**controller_identity_record_id** (string): Unique identifier (URI, DID, or legal entity identifier) enabling registry verification.

**controller_name** (string): Legal name of the controller entity.

**jurisdiction** (string): ISO 3166-1 alpha-2 or alpha-3 country code for controller's primary jurisdiction.

**rights_access_point** (string): URI or contact information for exercising data subject rights.

**lawful_basis_options** (array of strings): Legal bases available for processing (consent, contract, legal_obligation, legitimate_interest, vital_interest, public_interest).

**processing_purposes** (array of strings): Categories of processing purposes (service_delivery, analytics, marketing, research, etc.).

**scope_of_disclosure** (string): Risk category (child, youth, vulnerable, community, regional, national, international).

## 4.3 Optional Fields

**cir_publication_url** (string): Canonical URL for this CIR (typically the /.well-known/transparency location).

**notice_event_log_url** (string): Endpoint for querying notice state changes and material modifications.

**data_protection_officer** (object): Contact information for data protection officer if designated.

**policy_url** (string): Link to human-readable privacy policy.

**codes_of_conduct** (string or object): Reference to Convention 108+ or other applicable framework.

**processing_locations** (array of strings): ISO 3166-1 codes for data processing jurisdictions.

**recipient_jurisdictions** (array): For international scope of disclosure, destination jurisdictions for cross-border transfers.

**transfer_mechanism** (string): Legal mechanism for cross-border transfers (consent, adequacy, scc, bcr, etc.).

**surveillance_risks** (object): Disclosure of government access risks in recipient jurisdictions (when transfer_mechanism="consent").

## 4.4 Privacy Preference Signals

Controllers MAY declare support for privacy preference mechanisms through the **privacy_preference_signals** object:

**gpc_honored** (boolean): Whether controller honors W3C Global Privacy Control (GPC) signal. When true, controller commits to treating GPC as a valid opt-out of sale/sharing under applicable laws.

**gpc_scope** (array of strings): Specific processing purposes affected by GPC (e.g., ["marketing", "analytics", "third_party_sharing"]). Required when gpc_honored=true.

**dnt_honored** (boolean): Whether controller recognizes Do Not Track (DNT) browser signal.

**preference_center_url** (string): URI where individuals can manage granular privacy preferences without authentication.

**preference_binding** (string): How preferences are recorded (values: "browser_signal", "receipt_anchored", "account_based").

Example:

```
"privacy_preference_signals": {
  "gpc_honored": true,
  "gpc_scope": ["marketing", "analytics", "third_party_sharing"],
  "dnt_honored": false,
  "preference_center_url": "https://example.com/privacy/preferences",
  "preference_binding": "receipt_anchored"
}
```

**Rationale**: Privacy preference signals enable **transparency before identification**. Individuals can verify controller commitment to preference mechanisms before providing any personal data, supporting anonymous-by-default architecture.

## 4.5 Transparency Assurance and Trust Indicators

Controllers MAY declare transparency assurance levels and certification status through structured fields:

**transparency_assurance_level** (string): Level of transparency implementation per ISO/IEC 27560 MVCR-ANCR framework. Values:

- `L1_self_assertion`: Controller self-publishes CIR and notice.txt (baseline)
- `L2_registered`: CIR-ID registered with data protection authority
- `L3_ancr_signaling`: Anchored Notice Consent Receipts with cryptographic signatures
- `L4_active_state`: Real-time active-state signaling with certified notarization

**trustmark_certifications** (array of objects): Independent verifications and certifications. Each object contains:

- `trustmark_type` (string): Certification type ("habni", "tpi_r", "privacy_seal", "bcr_approval")
- `issuing_authority` (string): Name of certifying body or data protection authority
- `certification_id` (string): Unique identifier for this certification
- `issue_date` (string): ISO 8601 date of certification issuance
- `expiry_date` (string, optional): ISO 8601 date when certification expires
- `verification_url` (string): URI for independent verification of certification status
- `score` (number, optional): Numeric score for assessment-based certifications (e.g., TPI-R score 0-100)

**visual_trust_indicator** (object, optional): Machine-readable trust indicator for user agent rendering:

- `indicator_type` (string): Visual indicator type ("badge", "color_signal", "trust_score")
- `indicator_value` (string): Specific indicator (e.g., "green", "verified", "85")
- `indicator_url` (string): URI to official indicator icon or badge image

Example:

```
"transparency_assurance_level": "L3_ancr_signaling",
"trustmark_certifications": [
  {
    "trustmark_type": "habni",
    "issuing_authority": "Digital Transparency Lab",
    "certification_id": "HABNI-2025-001234",
    "issue_date": "2025-01-15",
    "expiry_date": "2026-01-15",
    "verification_url": "https://registry.transparencylab.ca/verify/HABNI-2025
-001234"
  },
  {
    "trustmark_type": "tpi_r",
    "issuing_authority": "Kantara Initiative",
    "certification_id": "TPI-R-2025-CA-567",
    "issue_date": "2025-02-01",
    "verification_url": "https://kantarainitiative.org/tpi-r/verify/567",
    "score": 87
  }
],
"visual_trust_indicator": {
  "indicator_type": "badge",
  "indicator_value": "verified_L3",
  "indicator_url": "https://standards.transparencylab.ca/badges/L3_ancr.sv
g"
}
```

**Rationale**: Transparency assurance levels create market differentiation for controllers implementing higher-assurance transparency practices. User agents (browsers, privacy tools) can render appropriate trust indicators, enabling informed individual choice. Regulatory dashboards can filter and prioritize enforcement based on assurance levels.

## 4.6 Global Privacy Rights Controls (GPRC)

Controllers MAY declare context-specific rights availability through the **global_privacy_rights_controls** array. GPRC enables mapping of data subject rights across the 72 transparency contexts defined by the ISO/IEC 27560 MVCR-ANCR framework:

**Transparency Context Matrix**: 3 data control vectors × 4 TATA levels × 6 legal bases = 72 distinct transparency contexts

Each GPRC entry is an object containing:

**context_id** (string): Unique identifier for this transparency context (format: "VECTOR_LEVEL_BASIS")

**data_control_vector** (string): One of:

- `personal_control`: Individual self-identifies and manages own data (SSI/DID paradigm)
- `data_protection`: Federated identification where third parties identify individuals
- `co_regulation`: ISO/IEC 27560 MVCR-ANCR profile with standardized notice-and-consent

**transparency_assurance_level** (string): One of L1_self_assertion, L2_registered, L3_ancr_signaling, L4_active_state

**legal_basis** (string): One of consent, contract, legal_obligation, legitimate_interest, vital_interest, public_interest

**available_rights** (array of strings): Rights exercisable in this context:

- `access`: Right to obtain confirmation and copy of personal data
- `rectification`: Right to correct inaccurate personal data
- `erasure`: Right to deletion (right to be forgotten)
- `portability`: Right to receive and transfer data in structured format
- `restriction`: Right to restrict processing
- `objection`: Right to object to processing
- `automated_decision_opt_out`: Right to opt out of automated decision-making

**rights_exercise_mechanism** (string): How rights are exercised in this context:

- `api`: RESTful API endpoint for programmatic rights exercise
- `web_form`: Human-accessible web form
- `email`: Email-based rights request
- `notice_receipt_anchored`: Rights exercise bound to notice receipt identifier
- `preference_signal`: Browser signal (GPC) treated as rights exercise

**rights_api_endpoint** (string, optional): URI for programmatic rights exercise when mechanism="api"

**response_timeframe** (string): ISO 8601 duration for controller response (e.g., "P30D" = 30 days per Convention 108+)

**authentication_required** (boolean): Whether authentication is required for rights exercise in this context

**verification_method** (string, optional): How individual identity is verified when authentication_required=true (e.g., "notice_receipt_id", "email_verification", "account_credentials")

Example GPRC configurations:

```
"global_privacy_rights_controls": [
  {
    "context_id": "CO_REG_L3_CONSENT",
    "data_control_vector": "co_regulation",
    "transparency_assurance_level": "L3_ancr_signaling",
    "legal_basis": "consent",
    "available_rights": [
      "access",
      "rectification",
      "erasure",
      "portability",
      "restriction",
      "objection",
      "automated_decision_opt_out"
    ],
    "rights_exercise_mechanism": "notice_receipt_anchored",
    "rights_api_endpoint": "https://api.example.com/rights/exercise",
    "response_timeframe": "P30D",
    "authentication_required": false,
    "verification_method": "notice_receipt_id"
  },
  {
    "context_id": "CO_REG_L3_LEGITIMATE_INTEREST",
    "data_control_vector": "co_regulation",
    "transparency_assurance_level": "L3_ancr_signaling",
    "legal_basis": "legitimate_interest",
    "available_rights": [
      "access",
      "rectification",
      "objection",
      "restriction"
    ],
    "rights_exercise_mechanism": "api",
    "rights_api_endpoint": "https://api.example.com/rights/exercise",
    "response_timeframe": "P30D",
    "authentication_required": false,
    "verification_method": "notice_receipt_id"
  },
  {
    "context_id": "DATA_PROT_L2_CONTRACT",
    "data_control_vector": "data_protection",
    "transparency_assurance_level": "L2_registered",
    "legal_basis": "contract",
    "available_rights": [
      "access",
      "rectification",
      "portability",
      "restriction"
    ],
    "rights_exercise_mechanism": "web_form",
    "rights_api_endpoint": "https://privacy.example.com/rights",
    "response_timeframe": "P30D",
    "authentication_required": true,
    "verification_method": "account_credentials"
  },
  {
    "context_id": "PERSONAL_CTL_L4_CONSENT",
    "data_control_vector": "personal_control",
    "transparency_assurance_level": "L4_active_state",
    "legal_basis": "consent",
    "available_rights": [
      "access",
      "rectification",
      "erasure",
      "portability",
      "restriction",
      "objection",
      "automated_decision_opt_out"
    ],
    "rights_exercise_mechanism": "preference_signal",
    "rights_api_endpoint": "https://api.example.com/rights/realtime",
    "response_timeframe": "PT1H",
    "authentication_required": false,
    "verification_method": "did_authentication"
  }
]
```

**GPRC Integration with Notice Event Logs**:

When individuals exercise rights through any GPRC mechanism, controllers SHOULD record the rights exercise event in the notice event log referenced by `notice_event_log_url`. This creates auditable transparency state changes tracked across all 72 contexts.

**Rationale**: GPRC transforms the CIR from static disclosure into **dynamic rights management infrastructure**. By explicitly mapping available rights to transparency contexts, this specification enables:

1. **Context-Aware Rights Exercise**: User agents can programmatically determine which rights are available based on current legal basis, TATA level, and data control vector
2. **Automated Rights APIs**: Privacy tools can invoke rights exercise endpoints without human intervention
3. **Regulatory Verification**: Data protection authorities can verify rights availability across all 72 contexts and track compliance at scale
4. **Preference Signal Integration**: GPC and other browser signals can be mapped to specific rights exercise in appropriate contexts
5. **Transparency Without Identification**: Rights exercise mechanisms can be designed for anonymous or pseudonymous verification using notice receipt identifiers

GPRC enables proportionate rights exercise: different legal bases and assurance levels provide different rights (e.g., erasure available under consent but restricted under legitimate interest with balancing test).

## 4.7 Example CIR (Minimal)

```
{
  "controller_identity_record_id": "CIR-CA-12345",
  "controller_name": "Example Service Ltd.",
  "jurisdiction": "CA",
  "rights_access_point": "https://example.com/privacy/rights",
  "lawful_basis_options": ["consent", "contract"],
  "processing_purposes": ["service_delivery", "analytics"],
  "scope_of_disclosure": "regional"
}
```

## 4.5 Example CIR (Cross-Border with Surveillance Risk Disclosure)

```
{
  "controller_identity_record_id": "CIR-CA-67890",
  "controller_name": "Global Cloud Services Inc.",
  "jurisdiction": "CA",
  "rights_access_point": "https://globalcloud.example/privacy",
  "lawful_basis_options": ["consent", "contract"],
  "processing_purposes": ["cloud_storage", "service_delivery"],
  "scope_of_disclosure": "international",
  "processing_locations": ["CA", "US"],
  "recipient_jurisdictions": [
    {
      "country_code": "US",
      "adequacy_status": "no_decision",
      "legal_regime": "Foreign intelligence surveillance legislation permits government access to data of non-US persons without notification"
    }
  ],
  "transfer_mechanism": "consent",
  "surveillance_risks": {
    "disclosed": true,
    "jurisdictions": {
      "US": "Data transferred to US cloud providers may be subject to lawful government access requests under foreign intelligence surveillance legislat
ion without individual notification."
    },
    "mitigation_measures": [
      "End-to-end encryption for data at rest",
      "Data minimization—only essential fields transferred"
    ]
  },
  "policy_url": "https://globalcloud.example/privacy-policy",
  "codes_of_conduct": {
    "legal_framework": "Council of Europe Convention 108+",
    "implementation_profile": "ISO/IEC 27560 Universal Notice Receipt Profil
e v1.0"
  }
}
```

# 5. Discovery Protocol

## 5.1 HTTP Request

Clients discover CIR by sending HTTP GET request:

```
GET /.well-known/transparency HTTP/1.1
Host: example.com
Accept: application/json
```

## 5.2 HTTP Response

Successful response:

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: public, max-age=86400

{CIR JSON content}
```

## 5.3 Error Handling

**404 Not Found**: Controller has not published CIR. Clients MAY check alternative location `/notice.txt`.

**403 Forbidden**: Access restrictions SHOULD NOT be applied to CIR (public accountability record).

**500 Internal Server Error**: Server-side failure. Clients SHOULD retry with exponential backoff.

### 5.4 Caching

CIR documents SHOULD include Cache-Control headers. Recommended: `Cache-Control: public, max-age=86400` (24 hours).

Clients SHOULD respect cache directives while also checking `notice_event_log_url` for material changes.

### 5.5 Content Negotiation

Servers MAY support multiple representations:

```
Accept: application/json
Accept: application/ld+json
Accept: text/html (for human-readable rendering)
```

## 6. Security Considerations

### 6.1 No PII in CIR

CIR documents MUST NOT contain personally identifiable information. CIR contains only controller accountability information, making public disclosure safe.

### 6.2 Controller Identification Verification

CIR-ID MUST be verifiable through authoritative registries to prevent controller impersonation. Implementers SHOULD:

- Cross-reference CIR-ID with legal entity registries (e.g., business registrations)
- Verify jurisdiction claims against authoritative sources
- Validate TLS certificates match controller_name when using HTTPS

### 6.3 Integrity Protection

While TLS is RECOMMENDED for CIR publication, it is not REQUIRED since CIR contains no confidential information. However:

- Controllers publishing CIR over HTTP SHOULD provide cryptographic signatures
- Clients SHOULD verify signatures when available
- Registry-based verification provides additional integrity assurance

### 6.4 Denial of Service

Controllers SHOULD implement rate limiting on `/.well-known/transparency` to prevent abuse:

- Reasonable rate limits: 100 requests/minute per IP address
- Aggressive caching reduces load
- CDN distribution recommended for high-traffic controllers

### 6.5 Registry Security

CIR registries operated by data protection authorities or other verifiers MUST:

- Authenticate controller identification before CIR-ID issuance
- Maintain audit logs of CIR updates
- Provide secure APIs for automated verification
- Implement DDoS protection

## 7. Privacy Considerations

### 7.1 Anonymous-by-Default Architecture

CIR publication enables **controller identification before individual identification**. This architectural principle:

- Allows individuals to verify controller identification anonymously
- Enables notice receipt generation without providing PII
- Supports surveillance-resistant transparency verification

### 7.2 No Authentication Required

CIR access MUST NOT require authentication. Requiring login would:

- Defeat anonymous discovery
- Create identification-before-transparency anti-pattern
- Introduce tracking risks

### 7.3 Transparency Without Surveillance

Public CIR registries enable regulatory oversight **without** creating individual surveillance infrastructure:

- Regulators verify controller transparency practices
- No individual-level tracking required for enforcement
- Registry queries reference controllers, not individuals

### 7.4 Privacy-Enabling Rights Exercise

**Terminology Note**: This specification uses "privacy-enabling" rather than "privacy-preserving" to reflect a fundamental paradigm shift. **Privacy-enabling** means individuals control their own data and identifiers without requiring corporate identification or permission (individual-centric data control). **Privacy-preserving** means companies protect data better on behalf of individuals (controller-centric data protection). The CIR infrastructure is regulatory capacity infrastructure for enforcement at scale, not compliance tools for companies.

The `rights_access_point` field enables individuals to exercise PII principal and data subject rights. Controllers SHOULD:

- Support privacy-enabling rights exercise mechanisms
- Allow anonymous rights requests where legally permissible
- Minimize authentication requirements for rights access

## 8. IANA Considerations

This document requests IANA to register the following well-known URI in the "Well-Known URIs" registry as defined by RFC 8615.

### 8.1 Registration Request

**URI suffix**: transparency

**Change controller**: IETF

**Specification document**: [this RFC]

**Related information**:

- ISO/IEC 27560:2025 - Structure of Personally Identifiable Information (PII) Processing Records
- Council of Europe Convention 108+ - Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data
- ISO/IEC 29100:2011 - Information technology — Security techniques — Privacy framework

**Status**: permanent

**Date registered**: [To be assigned by IANA]

# 9. References

## 9.1 Normative References

**[RFC2119]** Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997.

**[RFC8615]** Nottingham, M., "Well-Known Uniform Resource Identifiers (URIs)", RFC 8615, DOI 10.17487/RFC8615, May 2019.

**[ISO27560]** ISO/IEC 27560:2025, "Information security, cybersecurity and privacy protection — Structure of Personally Identifiable Information (PII) Processing Records".

**[CONVENTION108]** Council of Europe, "Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data", Treaty No. 223, 2018.

## 9.2 Informative References

**[ISO29100]** ISO/IEC 29100:2011, "Information technology — Security techniques — Privacy framework".

**[ISO29184]** ISO/IEC 29184:2020, "Information technology — Online privacy notices and consent".

**[EU2018-1725]** 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.

**[W3C-DPV]** W3C Data Privacy Vocabulary (DPV), https://www.w3.org/ns/dpv

**[RFC7519]** Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015.

# Appendix A. Implementation Guidance

## A.1 For Controllers

### Step 1: Generate CIR-ID

Obtain unique identifier from:

- Legal entity registries (business registration number)
- Decentralized identifiers (DIDs)
- Controller registry operated by data protection authority

### Step 2: Create CIR JSON

Populate required fields with accurate controller identification information. Ensure `rights_access_point` is operational.

### Step 3: Publish at Well-Known Location

Configure web server to serve CIR at `/.well-known/transparency` with `Content-Type: application/json`.

### Step 4: Register with Authorities (Optional but Recommended)

Add, or Submit where applicable,  CIR-ID to data protection authority registration or registry for verification and public listing.

### Step 5: Maintain Notice Event Log

Track material changes to processing practices. Provide queryable endpoint at `notice_event_log_url`.

## A.2 For Individuals and User Agents

### Step 1: Discover CIR

Before providing data, retrieve controller CIR:

```
GET https://example.com/.well-known/transparency
```

**Step 2: Verify Controller Identification**

Cross-reference `controller_identity_record_id` with public registries.

**Step 3: Generate Notice Receipt (Optional)**

Combine CIR with context (timestamp, notice type, legal basis) to create bilateral notice receipt.

**Step 4: Exercise Rights**

Use `rights_access_point` to submit access, rectification, erasure, or portability requests.

### A.3 For Regulators

**Step 1: Establish CIR Registry**

Operate public registry of verified CIR-IDs with controller identification information.

**Step 2: Automated Verification**

Crawl `/.well-known/transparency` endpoints to verify controller transparency compliance.

**Step 3: Enforce Transparency Requirements**

Identify controllers lacking CIR publication or with incomplete transparency information.

**Step 4: International Coordination**

Federate CIR registries across jurisdictions for cross-border transfer verification.

---

## Appendix B. Comparison with Existing Mechanisms

### B.1 vs. Privacy Policies

**Traditional Privacy Policies**:

- Unstructured HTML documents
- No standard location
- Human-readable only
- Difficult to verify or compare

**CIR at /.well-known/transparency**:

- Structured JSON format
- Standard well-known location
- Machine-readable with human rendering
- Automated verification possible

### B.2 vs. robots.txt

`robots.txt` provides precedent for root-level disclosure files. However:

- robots.txt governs crawler behavior (technical)
- CIR governs data processing (legal/privacy)
- Both benefit from standardized locations

### B.3 vs. security.txt (RFC 9116)

`security.txt` (RFC 9116) uses `/.well-known/security.txt` for security contact disclosure. This specification follows similar pattern:

- Standard well-known location
- Machine-readable structured format
- Public accountability information
- No authentication required

---

## Appendix C. Future Extensions

### C.1 Signed CIR

Future work may specify cryptographic signatures for CIR integrity:

- JSON Web Signatures (JWS) per RFC 7515
- Verifiable Credentials per W3C specification
- Integration with controller public key infrastructure

### C.2 Multi-Controller Coordination

For complex processing involving multiple controllers:

- CIR chaining for third-party disclosure transparency

- Joint controller CIR references
- Processor transparency through controller CIR links

### C.3 Dynamic State Signaling

Real-time transparency state changes:

- Server-Sent Events or WebSockets for live notice event log
- Active-state signaling for high-assurance contexts
- Push notifications for material changes

## Acknowledgments

This specification builds on years of work by the Kantara Initiative Consent & Information Sharing Work Group, the Digital Transparency Lab, and the ISO/IEC JTC 1/SC 27/WG 5 community.

Key contributors to the underlying Controller Identification Record concept and ISO/IEC 27560 profile development include: Mark Lizar (Digital Transparency Lab), Sal D’Agositno (IDmachines) and the ANCR Working Group participants.

The well-known URI framework defined in RFC 8615 by Mark Nottingham provided the foundation for this standardized discovery mechanism.

## Authors' Addresses

**Mark Lizar**

Digital Transparency Lab

Email: mark@transparencylab.ca

URI: https://transparencylab.ca

**Document History**

**draft-lizar-transparency-wellknown-00**: Initial submission, December 2025