ANCR Digital Transparency Performance Scheme: Parts 1 and 2

Conformity & Compliance Assessment v0.9.2

ANCR refers to an Anchored Notice & Consent Receipt, it is a record that is generated using the Transparency Performance Indicator assessment, which provides a standard measure of operational performance of the present PII Controller's security and privacy session information.

Editor(s):

- Mark Lizar, WG Co-Chair, WG Editor

Contributors:

- Sal D'Agostino, WG Chair
- Sharon Polsky
- Paul Knowles

Reviewers:

- Gigi Agassini, ANCR WG Secretary

IPR Option:

This ANCR Record Specification is required to be open, as specified under a Patent & Copyright: Reciprocal Royalty Free with Opt-out to Reasonable and Non-discriminatory (RAND) license agreement at the Kantara Initiative for submission to ISO/IEC SC 27 WG 5.

Any derivative use of this specification must be in conformance with the associated transparency Code of Conduct[1], be open and free and not create any dependency that limits or restricts the use, accessibility, and availability of digital transparency or the ability for the PII Principal to provide and manage their own consent.

Suggested Citation: (upon WG approval)

ANCR Digital Transparency Performance Scheme, Part 1 & 2 v1.0

NOTICE

This specification relies on (open access to) ISO/IEC 29100 Security and privacy techniques, to generate a notice receipt, which is stored in an ANCR consent record format for conformity assessment as specified in the Kantara Initiative Consent Receipt v1.1.[2]

Conditions for use

License Condition: This specification is solely used for assessing conformance to the Transparency Code of Conduct (Appendix C), for implementing the Council of Europe 108+ Chapter III, Rights of the Data Subject, Section 1 Transparency, and modalities, Article 14, 1 – 8. This Transparency Code of Conduct is internationally representative of notice and consent legal and social requirements. It can be represented today in the form of privacy policy links, physical signage, digital cookies and security or privacy notices. These are found when accessing public and digital service spaces, in all domains and jurisdictions, and are to be referenced as practices, which MUST implement, or support the implementation of this Transparency Code of Conduct for transparency modalities.

[1] Transparency Code of Conduct, to implement Transparency Modalities – Appendix C.

[2] Consent receipt v1, CISWG Kantara Initiative https://kantarainitiative.org/download/7902/

Dear reader,

Thank you for downloading this publication prepared by the international community of experts that comprise the Kantara Initiative. Kantara is a global non-profit 'commons' dedicated to improving trustworthy use of digital identity and personal data through innovation, standardization, and good practice.

Kantara is known around the world for incubating innovative concepts, operating Trust Frameworks to assure digital identity and privacy service providers and developing community-led best practices and specifications. Its efforts are acknowledged by OECD ITAC, UNCITRAL, ISO SC27, other consortia and governments around the world. "Nurture, Develop, Operate" captures the rhythm of Kantara in consolidating an inclusive, equitable digital economy offering value and benefit to all.

Every publication, in every domain, is capable of improvement. Kantara welcomes and values your contribution through membership, sponsorship and active participation in the working group that produced this and participation in all our endeavors so that Kantara can reflect its value back to you and your organization.

Abstract

In context of processing personally identifiable information a PII Principal is not able to see who is processing their data or is not notified when their data is disclosed. As a result, today, the Individual is not able to trust the use of digital identity technologies and digital trust.

- At this time there is little transparency over required digital security and privacy online. This is largely due to outdated record
- Transparency varies from service to service and as a result it is impossible for people to see and trust how they are being identified as well as what is happening with their own data.
- Even so, the requirement to identify the legal entity and the accountable person to the PII Principal is a universal requirement for all data processing activities unless explicitly derogated by legislated law or policy for a specific legal justification and context.

If the PII Principal is not able to see how PII (Personally Identifiable Information) is shared, disclosed, or managed it is not possible to make the choice to trust the service processing PII.

For people, consent by default requires assurances that personal data is being processed and transparency in a meaningful and operationally manner Standard and operational transparency enabled by standardized schema, and record formats (Notice Receipts) so that people keep and own to control personal information and private AI. what can make consent meaningful by default. To create and scale trust in digital contexts a Digital Transparency Code of Conduct is introduced to simplify and clarify requirements and the use of CoE 108+ Chapter 1 Transparency Modalities, which is mirrored in the GDPR Article 12, 'Transparent information, communication and modalities for the exercise of the rights of the data subject'.

Scheme Applicability

1. All data processing must have a record of notified processing activity. In order to be digitally transparent, unless required not to be by legal derogation. In such an instance, the processing must be transparent to the appropriate regulatory authority, according to the context of processing.
2. This applies to all services and every stakeholder, PII Controller, PII Processor, PII Principal's, the PII Co-Regulating Authority and delegates.
3. All processing with consent requires a record of the privacy notice and privacy policy link, which in this document is referred to as a Notice Receipt, also known as the ANCR record of consent, and referred to as a consent record in ISO/IEC 27560 Consent record information structure.
4. Records and receipts provided as specified in Convention 108+, Art 31 Record of Processing Activity (RoPA). The consent receipt is effectively a digital twin, which is a mirrored notice and consent record, which is also held by the individual. This Record can then effectively become the authoritative consent record.
5. A Notice Receipt can be created by any stakeholder to identify a PII Controller.
6. An Anchored Notice and Consent Receipt can be used as a record of consent to access data subjects' rights for example, and/or to test and assess the operational performance of PII Controllers' digital privacy in digital contexts.

Part 1 of the scheme introduces 4 Transparency Performance Indicators; these are used to measure and rate the conformance of transparency. In Part 2 of the scheme (in the

Appendix A) a transparency information request is sent to the controller to; a) test the controller information and, b) measure how compliant the performance of digital transparency is, to both legal expectations and the personal privacy expectations of PII Principal.

1 TERMS & DEFINITIONS

Normative to Council of Europe, Convention 108+,

The normative language for the TPI Scheme is defined by Convention 108+ the commonwealth privacy convention the GDPR (General Data Protection Regulation) mirrors. Convention 108+ was created to establish a set of principles and rules to effectively safeguard personal data and facilitate cross-border data flows

Normative terms for roles defined in national law are mapped to the roles which are defined according to an international adequacy baseline.

ISO/IEC 29100 is also normative, this security and privacy framework standard maps terms in the standard itself, for example PII Principal is mapped to the Data Subject.

The ANCR Record Framework is used to specify Transparency Performance Indicators (TPIs) and is based on the consent receipt work where roles are mapped to standards and laws.

Stakeholder	Conv 108+	GDPR	ISO/IEC 29100	PIPEDA
Data Regulator				
Data Subject	X	X	PII Principal	
Data Controller	Controller	X	PII Controller	Organization
Data Processor	Processor			
Joint-Controller				
Sub-Processor				
Data Subject	X, Individual	X	PII Principal	Individual

(compliance roles, mapped to be interoperable within any data privacy framework)

Roles in this document refer to the relationship between the Individual and any digital service.

Introduction

Transparency Performance Indicator's (TPIs) are introduced here as the object of conformity to capture the presentation of PII Controller (Credential) information, and to determine the operational capacity of the information in conformance Conv 108+ and personal expectations.

The TPIs are used to create an ANCR (Anchored Notice and Consent Receipt) Record, which is presentable as a 'proof of notice' (or knowledge) claim, the object for both conformity, and compliance assessments, presented in this scheme.

The TPI scheme, to test the performance of digital transparency with a privacy request. This is used to determine how dynamic the performance of transparency and consent is for using data subject rights, independently of the service provider, and relative to context.

The TPIs presented pinpoint 4 metrics that can be used to measure the conformance of transparency and the integrity of consent in the relevant data capture context.

The TPIs assess the operational capacity of the *required and presented* PII Controller Identity and Contact attributes, or meta-information. The TPIs measure the existence and performance of the publicly required digital service information. The TPIs check digital components, identifying the governance model, authority, and security framework to assure the validity of privacy state in an online service context. Providing privacy risk assurance for people.

The ANCR record produced from a TPI Assessment captures digital governance and surveillance context. Capturing at the point of presentation PII Controller Identifiers, privacy rights access point(s), and importantly, under which digital governance framework personal data processing is being governed.

The ANCR record, in which the PII Principle is the holder and controller of this record, can be presented as a micro-notice claim and used as a credential to engage PII Controller privacy services and track the PII Controller performance.

Most assessments for conformance of privacy information or services are mapped to analogue legal requirements which measure response times in days, out of technical context. TPIs all measure how dynamic privacy service information is in context, and provide a rating, from -3 to +1, in which +1 is for a Dynamic, in context transparency performance indicator. This introduces the concept of a shared *active privacy state transparency*, comprised of the signal that indicates if the privacy as expected in context.

Why was this specification written?

At the time of writing this specification, transparency and consent is governed predominately by commercial governance frameworks that utilize digital identity management technologies to identify people. At the same time the associated services do not identify themselves in a standard way online, which is neither compliant nor conformant, presenting critical cybersecurity risks.

Individuals are forced to give up digital privacy to access analog privacy services online. All the records of digital relationships are kept by services, (if they keep records at all). Without our own records of digital relationships Individuals are not able to access the information necessary to measure privacy and security and meet a threshold for notice and a basis for processing, including and importantly consent.

These risks and harms are exacerbated when PII Principals use privacy services online. PII identifiers, by default, are captured and collected at an attribute level (known also as meta-data). This means individuals must relinquish control over these attributes and digital privacy, to access online services. These "security" technologies themselves are used to profile and track data subjects presenting systemic challenges to accessing privacy in a meaningful way for the PII Principal.

The second systemic obstacle is that individuals do not have their own records of digital identity relationships. The lack of records prevents people from being able to exercise rights.

A notice receipt and consent record address this systemic and root challenge, with proof of notice, which is required to be present as evidence consent. This Transparency Performance Scheme is a first step towards the evidence of consent missing in today's online services.

Why Transparency Performance Indicators?

Currently, there is no way for people to see who is tracking them and to understand how digitally exposed one is, in any given surveillance context, whether physical or digital.

TPIs assess when the notice is presented, if the notice information provided is contextually relevant, if the contact information is fake or not, is it usable reciprocally, and proportionally, and if a digital service can represent policy and security required for digital privacy. The information and understanding gained from applying these indicators is a necessary precondition for any processing of personal data and meaningful consent.

Digital transparency requires standard purpose specification to include who benefits, how they benefit, and where the benefit and value originates. This is required and unfortunately mostly missing security information. It is assessed and presented in a standard credential, record, and receipt format in the Scheme. Without a standardized notification and presentation format to govern identity management, it is difficult for a Data Subject to make a trust decision, and impossible in a multi-service context, limiting the capacity to trust any services provided online.

The invisible risks need to be presented relevant to the context to allow an informed choice about whether to consent, withdraw consent, or even pause consent to a service, and/or to stop tracking for a particular private context.

This scheme and assessment make these risks transparent. TPIs conformity and compliance assessment for digital transparency dramatically improves safety, security, privacy usability, and awareness for all stakeholders.

About the Scheme

The TPI Scheme presented here is scoped to specify the public digital transparency at a self-assurance level referred to as level 0 transparency assurance in the ANCR Framework. The framework includes:

A conformity and compliance assessment scheme, implemented in 2 parts to generate a full operational transparency report.

- TPI Scheme 1 Part 1 - Conformance
  - Initial test to diagnose the operational capacity of privacy services in any specific context.
- TPI Scheme 1 Part 2 – Compliance (found in Appendix A)
  - Specifies an example operational transparency compliance performance test, in which the transparency is tested by generating a privacy rights-based request, to access privacy services.

Part 1 refers to conformance with digital identifier elements of the PII Controller required to be presented to initiate a session and is the body of this document.

Part 2 is Appendix A and uses the ANCR record to audit the Adequacy of the captured practice as specified in the Council of Europe, Conv. 108+. Article 14, Transparency Modalities.

The 4 Transparency Performance Indicators capture transparency and data capture practices in context and are used to test the self-asserted information for its operational usability.

These 4 TPIs and Scheme 1, Part 1, and Scheme 1 Part 2 can be used together with the Appendices for its public interest application, as well as for the demonstration of an Controller credential encompassing the TPIs and associated assessment. The scheme is directed at providing a basis for required public security and privacy transparency assurance.

TPIs specified focus is on the initial point of contact. This includes the publicly required information that MUST be provided and refers to the PII Controller Identity and Contact information, which is required in all legal privacy instruments. Transparency, in this regard, is a universal requirement, and required for not only as free, prior, and informed consent to scale as digital privacy online but also a means of governing and providing trust in authority.

The TPIs here are used to assess session-based data capture and self-asserted information by organizations to specify a public level of trust assurance that is provided in an online context.[3]

[3]Note to reader: The ANCR Record Framework presents 4 levels of transparency assurance for PII Controller (Notice) Credentials, which can be use in 3 vectors of digital governance; 1. Personal data control 2. Data Protection 3. Co-regulation, which is what is assessed in this document at assurance level 0.

TPI 1 - Measuring the Timing of PII Controller Identity Notification:

This TPI captures ***when*** the Controller's legal entity and accountable Privacy Officer (digital identifiers) provide notice of their identity. This is measured to see if the notice is delivered

i) Before,
ii) At the time of,
iii) During, or
iv) After

Personally identifiable information is captured.[3]

By assessing dynamic and operational transparency, as opposed to static, infrequent information, it provides a way for an individual to assess if they can trust a service or not. This is also assessing compliance with Article 14.1, and specifically defined in Article, 15 1, a) and b)

Commented [SD1]: Reference to be inserted

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller;

(b) the contact details of the data protection officer;

TPI 2 - Measures Required Data Elements

This TPI captures whether the required security and privacy attributes are provided,[4] These are required to provide the PII Controller information for all accountable parties. Namely ***who*** and ***what*** information about them is legally required. In "all" cases, there is a requirement for a Notice of who is processing your data, who is accountable, and the privacy contact information for access to personal information and rights, and is also required. [Art 14.1]

[4] This is the most common legislated privacy element in the world, required and mappable to all privacy legislation and instruments. (ISTPA 2007)p.64

A *first-time notice* must exhibit two (2) factors (2FN), 1) is the notice adequate as notice of risk, and 2) are the practices relating to permissions permitted by the purpose, accepted, which can then be used as proof of notice by the data subject.

Thes following Digital Privacy transparency elements are the minimum required to operationalize transparency and accountability.

i) Legal Entity Identity Name,
ii) Address, Contact information
iii) Name or role of Data Privacy Officer (or the authoritative owner and Accountable Person (AP) in charge of that legal entity.
iv) Privacy services access and contact point information.
v) Privacy or other policy governing the processing of personal information.
vi) Transparency information before use
    a. Digital governance framework
    b. Legal Basis for Purpose of initial Processing of PII
    c. Recipients or categories of recipients if any
    d. Transfer of data on networks out of Country, to a 3rd Country,
    e. The existence of adequacy,
    f. Existence of safeguards, where to get a copy of them, or where they have been made available.[5]

TPI 3 - Measure of Transparency Accessibility

This TPI measures the performance of transparency in terms of ***accessibility*** to the information in TPI 2. For example, is the information readily available, ideally prior to the digital session and capture of PII. For example, is TPI-2 information presented in a pop-up notice at the initiation of a digital service session, or is it required to click a link, e.g., to a privacy policy, and then access additional link. , Is the operational transparency information on the first screen, or is it at the bottom reached only after scrolling multi-pages, with links not highlighted, and not accessible to children or parents.

In this way TPI 3 measures Informational accessibility, is a key transparency metric that indicates if the context is digital privacy capable of being inclusive and accessible and trustworthy. This measure is extended to include the exercise of rights on the part of the PII Principal to determine how adequately Controllers respond.

[5] An international repository would be an ideal for framework when accessing thes first-time sign or notice.

TPI 4: A Measures security information integrity

This TPI captures the relevant digital certificates, (e.g. x.509), or security token (e.g. JOSE) keys to compare the security meta-data, and policy objects against the required information in TPI 2. It also checks for consistency and continuity in the security provided and is it adequate for the task. E.g., does an SSL certificate Organization Unit field and Jurisdiction fields match the captured legal entity information? How do the policy and jurisdiction there relate to other beneficial entities? Importantly does this align with the policy expectations of the person?

TPI Metrics

Transparency Performance Rating

The TPI Rating system is designed to measure dynamically the operational transparency and performance of the required security and privacy information and its usability. The scale applied penalizes bad behavior more than it rewards conformance and compliance from +1 "good" to -3 "bad". These are presented one by one and then in a table for comparison followed by an example in the next section.

For TPI 1:

- +1 refers to the existence of a technical framework and PII Controller transparency ***prior*** to the initiation of a session. This provides security-based trust assurances for the data subject.
- 0 refers providing dynamic transparency in context ***at the start*** (which is at the time of collection), including purpose and other required disclosures,
- -1 refers to where the legally required information is presented at some point in the session.
- -2 refers to the provision of low quality legally required information.
- -3 refers to the provision of non-operable, non-compliant, unusable transparency and digital privacy related information.

For TPI 2

- +1 is given for each of the Controller information of the elements
- -3 if the information is missing.

For TPI 3

- +1 for meeting legal requirements for responsiveness for each of the required PII Controller information categories.
- -2 for response but not within legal requirements
- -3 if information unavailable

For TPI 4

- +1 for the contextual integrity of each the security features
- 0 if information available but not immediately or easily accessible
- -3 for each integrity mismatch

Table 1: Transparency Performance Indicator Record Ratings

The following shows how TPIs work together as timing is relevant to all the TPIs.

Rating	TPI 1 Timing of Notice	TPI 2 Content of Notice	TPI 3 Access to Content	TPI 4 Security Integrity
+1 (assured)	Before Transparency of control - governance required information	Controller Information - Credential is registered and present	Controller identity is presented prior to data collection	Security demonstrated prior to data collection (browser and digital wallet based)
0 (contemporaneous assurance)	Just in time, At the time of	Notice/credential is presented just in time (automated check and first-time notice)	Embedded as a credential linked to authoritative registries.	Is assured -e.g., certificate is specific to and matches controller and context
-1 (analogue assurance - online)	During	Controller information is accessible during collection	PII Controller Identity prominently displayed on first view – prior to processing first page of viewing, the assessment question would be	not-specific to controller - does not match jurisdiction
-2 - (not mandatory in flow)	Available	Controller information is linked	Link not presented	E.g., available but does not match OU or CN
- 3 (non-operative)	After	Controller information not present	Identity or credential is not accessible in context - e.g., two or more screens away, or privacy contact is mailing address and non-operative in context of data collection.	Valid issuer, cryptography, expiration, or policy NOT provided.

Table 2: Transparency Performance Indicator Record Rating Example

Field Name	Field Description	Requirement:	TPI 1	TPI 2	TPI 3	TPI 4 Certificate or Key
Notice Location	Location of where was read / observed	MUST	At time of 0	Present +1		Match +1
PII Controller Name	Name of presented organization	MUST	At time of 0	Present +1	Responsible entity verified +1	Match (CN, OU) +1
PII Controller Address	Physical organization Address	MUST	At time of 0	Present +1	Location accessible +1	Not match -3
Privacy Contact Point	Location / address of Contact Point	MUST	Not present -3	Not Present -3	Point of contact verified +1	Not match -3
Privacy Contact Method	Contact method for correspondence with PII Controller	MUST	Information linked -1	Present +1	Response in required time +1	Match +1
Session key or Certificate	A certificate for monitored practice	MUST	At time of 0	Present +1	Not Expired +1	Not contextually valid -3

Summary

In summary, Transparency Performance Indicators (TPIs) are specified here for people to use in context in combination with out of session elements, independently of service providers to gain an understanding of digital identifier relationships. TPIs are digital transparency tools used to self-determine how much a service in context can be trusted.

These TPIs are designed to work with open standards, and licenses, e.g. ANCR WG royalty free license, and open-source software to provide adequate, and scalable Transparency conformance. Transparency tools are required to be open in multiple ways so that people can use and create records they can own and keep across and independently of service providers. It is a cornerstone of agency that the scheme puts in place.

TPI 1 is a measure of trust, so that when asked, "Do you trust (accept) a service", you necessarily know who is processing your data before, during or after." Overwhelmingly people indicate trust would be higher. if notified prior to data capture, which only makes sense.

TPI 2 is the legally required attributes, present and available. Are they machine readable

TPI 3 is an indicator of how accessible, and inclusive, digital transparency is. Are the transparency attributes machine readable.

TPI 4 validates for the individual if security "matching the controller jurisdiction" to addresses a critical cross-border security challenge widely overlooked today.

This is a 1.0 document; we look forward to its evolution.

APPENDIX A: TPI COMPLIANCE ASSESSMENT SCHEME PART 2

A.1 Operational Transparency Assessment

The following describes an assessment using the TPIs to means Operational Transparency and assurance.

Most often for the PII Principal there are missing, but required for operational digital governance, identifying attributes, controlled, and held by PII Controllers with commercial interests. This scheme looks to systemically capture and control these attributes as digital commons assets turned into public infrastructure to support Operational Transparency.

i) Transparency is required to be available in context, i.e., during the time when PII is obtained (found in Transparency Statement or Privacy Policy).[6]
   a. Time period data stored.
   b. Existence of rights/controls to access and rectify.
   c. Existence of right to manage consent.
   d. Existence of right to lodge a complaint with a Data Protection Authority (DPA).
   e. Whether processing is based under a statutory, or contractual context, or whether necessary for entering a contract, if the PII is obliged, and the consequences of failure to provide this data.[7]
   f. Existence of
      i. AI, or any automated decision-making technology
      ii. Digital identity management surveillance technologies
      iii. Any profiles, or graphs generated
      iv. Meaningful information about the logic involved
         1. It significance in overall policy or processing
         2. Expected consequences for and to PII Principal - Data Subject

[6] A second factor notice must be linked to the first notice receipt/record to provide proof of notice and state.

[7] This is missing from CoE 108+ - but required element to include in the Code of Conduct.

APPENDIX B: TPI ASSESSMENT GUIDANCE

The TPI Rating system is designed to measure the operational performance of the information, for example if only a mailing address is provided for a privacy contact on a website, this is considered non-operable according to the context. This means that privacy access and specific information is not retrievable in the context of data collection. The TPIs measure adequacy and demonstrate non-performance by PII Controllers as a form of data co-governance.

The associated Conformity Assessment: uses the open ISO/IEC 29100 security framework for generating interoperable records and receipts of data processing activity, according to transparency in context.

B.1 TPIs are captured in sequence

a. TPI 1 measuring the point when the individual is notified versus when personal information/digital identifiers are collected and processed. The scheme starts by capturing the timing of notice presentation in relation to first data capture, and first contact.[8]

b. TPI 2 measuring the contents of the notification for required PII Controller digital attributes that correspond to the physical brick and mortar attributes specified in privacy, security, safety, and surveillance legislation. This is the PII Controller identity and entity information and access point.

c. TPI 3 measures how usable are the contents (information record) of the PII Controller entity, and its identity information and access point.

d. TPI 4 validates the coherence of cybersecurity information versus the digital transparency information capturing the SSL certificate and/or tokens/keys and associated meta-data (e.g. object identifiers, and certificate policies).

Combined, these TPIs provide an overall Indication of the operational state of digital privacy.

[8] Flows for return visits can make use of receipts that capture the state of the relationship on first contact, and record and maintain any change of state thereafter for any use by any controller, including joint controllers, sub-controllers, processors, and sub-processors.

B.2 TPI – Scheme 1, Part 1(S1-P1) metric logic

Rating - Instruction	TPI 1 Timing (with regards to processing)	TPI 2 Required Information	TPI 3 Accessibility	TPI 4 - Digital Security
+1 (assured)	PII Controller credential is displayed, using a standard format with machine readable language, and linked, for example, in an http header in a browser	The Controller is discoverable prior to session (out of band) in a machine-readable format: 1.Controller Registry 2.A client-side record of processing (via a wallet or browser)	Controller identity is presented prior to data collection	Security is required prior to collection (digital wallet based)
0 (dynamic assurance)	PII Controller Identity or credential is provided in first notice	Credential is presented just in time (automated check and first-time notice)	Embedded as a credential and dynamically available upon access (almost just in time)	is assured -e.g., certificate is specific to and matches controller and context
-1 (analogue assurance - online)	The Controller Identity, or screen with the Controller Identity is one screen and click away. For example, the privacy policy link in the footer of a webpage	controller information is accessible (not presented) during collection	PII Controller Identity prominently displayed on first view – prior to processing first page of viewing	not-specific to controller - does not match jurisdiction
-2 - (not mandatory in flow)		Controller Credential information is linked during collection	is linked not presented	does not match ou
-3 (non-operative)	PII Controller Identity is not accessible enough to be considered 'provided'	Controller information not present	Identity or credential is not accessible in context - e.g., two or more screens of view away, or privacy contact is mailing g address and non-operative in context of data collection.	It is not a valid, secure, or recognized provider. Not security operational (proving nonreciprocal security assurance)

532

B.3 1.2. Table 2: ANCR Record Schema Example

534 This appendix is an example of a notice record and the schema and can be used as a
535 template for the information record, rating, and analysis.

536

FIELD NAME	FIELD DESCRIPTION	REQUIREMENT: MUST, SHALL, MAY	FIELD DATA EXAMPLE
Notice Location	Location the notice was read/observed	MUST	Walmart.com (actual link)
PII Controller Name	Name of presented business	MUST	Walmart
Controller Address	The physical address of controller and/or accountable person	MUST	1940 Argentina Road Mississauga, Ontario L5N 1P9
PII Controller Contact Type	Contact method for correspondence with PII Controller	MUST	Email, phone
PII Controller-Correspondence Contact	General contact point	SHALL	Privacy@org.com
Privacy Contact Type	The Contact method provided for access to privacy contact	MUST	Email, or other
Privacy Contact Point	Location/address of Contact Point	MUST	Org.com/privacy.html
Session Certificate	A certificate for monitored practice	Optional	TLS, Transparency, Policy (OID) Context

APPENDIX C: DIGITAL TRANSPARENCY CODE OF CONDUCT

These digital transparency code of conduct rules coincide with the TPIs presented and reference the international adequacy requirements for transparency required for digital identifier management. In Report on the Adequacy of Digital Identity Governance for cross border transparency and consent:

PII Controller must:

1. Provide their PII Controller Notice Credentials, before or at the time of processing personal information (TPI 1), Article 14.1
2. PII Controller credential information must be accessible
3. PII Controller credential information must be operationally capable for access to rights with evidence of notice & consent
4. The security context must match the controller's jurisdiction where it is assumed PII is processed

Endnotes

[1] Lizar, M, Pandit, H, Jesus, V, "Privacy as expected Consent Gateway", Next Generation Internet (NGI) Grant [Access July 4] privacy-as-expected.org/