Anchored Notice and Consent Receipt (ANCR) Transparency Performance Indicator (TPI) Conformity & Compliance Assessment Scheme 1, Parts 1&2, v0.9

Transparency Performance Indicators are specified as a standard measure of the operational performance of the presented PII Controller security and privacy information.

Editors:

- Mark Lizar, WG Editor

Contributors:

- Sal D'Agostino, ANCR WG Chair

Reviewers:

- Gigi Agassani, 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 Specification v`0.9 ANCR TPI Conformity & Compliance Assessment Scheme 1, Part 1 & 2

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]

Use in these conditions.

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 forms 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, are to be referenced as practices, which MUST implement, or support the implementation of this Transparency Code of Conduct for transparency modalities.

This document has been prepared by participants of Kantara Initiative Inc ANCR-WG. Permission is hereby granted to use the document solely for the purpose of implementing the Specification for public benefit. No rights are granted to prepare derivative works of this Specification. Entities seeking permission to reproduce this

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

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

document, in whole or in part, for other uses must contact the Kantara Initiative to determine whether an appropriate license for such use is available.

Implementation or use of this document may require licenses under third party intellectual property rights, including without limitation, patent rights. The Participants and any other contributors to the Specification are not and shall not be held responsible in any manner for identifying or failing to identify any or all such third-party intellectual property rights. This Specification is provided "AS IS," and no Participant in Kantara Initiative makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third-party intellectual property rights, or fitness for a particular purpose. Implementers of this Specification are advised to review the Kantara Initiative's website (Kantara Initiative: Trust through ID Assurance) for information concerning any Necessary Claims Disclosure Notices that have been received by the Kantara Initiative Board of Directors.

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 elements online.
- 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, security by default requires assurance to see when personal data is being processed to operationally be transparent. Standard and operational transparency captured in records (Consent Receipts) people keep and own is what can makes 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 be 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 becomes 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 Common wealth privacy convention the GDPR (General Data Protection Regulation) mirrors. . Originally convened 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	Quebec
Data Regulator					
Data Subject		X	PII Principal	Data Subject	
Data Controller	X	X	PII Controller	Organization	Person in charge of protecting personal information (PICPPI)
Data Processor					
Joint-Controller					
Sub-Processor					
Data Subject		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 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 provides 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 service online . While all the records of the digital relationships are kept by services, (if they keep records at all). Without our own records of digital relationships Individuals are not able to be empowered .

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 their digital privacy, to access online privacy services. These "security" technologies themselves are used to profile and track data subjects presenting systemic challenges to accessing privacy services 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. Preventing people from being able to exercise rights.

A notice receipt and consent record address this systemic and root challenge, with a proof of notice, which is what is required to present evidence consent. Evidence of consent that is 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, physical or digital.

TPIs assess if the notice information provided is operational, if the contact information is fake or not, if a digital service is even capable of the security required for digital privacy to be trust capable. requirement to be notified and have an understanding of (digital) risks before making decisions. It is a necessary precondition for meaningful consent.

Digital transparency requires standard purpose specification to include who benefits, how they benefit, and where they benefit from, is extremely important. This is required but missing security information that's is made assessed 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 in an online context.

The invisible risks need to be presented relevant to the context to make an informed choice about whether or not to consent, withdraw consent, or even pause consent to a service, to stop tracking for a particular private context

A challenge addressed with the use of this assessment, which makes these risks transparent.

TPIs conformity and compliance assessment for digital transparency dramatically improves the 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 assurance level referred to as level 0 (digital commons) 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 required to be presented to initiate a session, and is the body of this document, while TPI Scheme 1, Part 2, is Appendix A, which is the next set of TPI elements audited for compliance with international digital governance transparency requirements referenced in Conv. 108+. Article 14, Transparency Modalities.

The 4 Transparency Performance Indicators h 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 Guidance – Appendix –, for the public interest application, as well as the demonstration of this project's use of the digital credential. In this regard, this TPI Scheme directed at required public transparency level of risk 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 privacy legal instruments. Transparency, in this regard, is a universal requirement, and required for free, prior and informed consent to scale as digital privacy online.

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]

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]

[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.

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)

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 operationally the transparency information and identify the accountable party. Namely ***what*** information 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 is required to be *provided*. [Art 14.1]

Specifically, a first-time notice must include 2 factors, 1) is the notice adequate as notice of risk. 2) is the practices relating to permissions permitted by the purpose, accepted and can be used as proof of notice by the data subject.

These 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 Governance Policy Governing the processing of personal information.

[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

vi) Transparency before use
   a. Digital Gov-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. (note)

*** edited to here ***

TPI 3 - Measure of Transparency Accessibility

This TPI measures the performance of transparency in terms of ***accessibility***by 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 – for Informational accessibility, is a key transparency metric that indicates if the context is digital privacy capable of being inclusive and accessible and trustworthy.

TPI 4 - Measures security information integrity

This TPI captures the (Secure Socket Layer/Transport Layer Security) SSL/TLS (e.g. 1.3) certificate or security keys (e.g. JOSE) to compare its security meta-data against the required information in TPI 2. This is very much along the lines of Certificate Transparency but looking specifically at whether the security certificate conforms to the ANCR Record profile policy. It also checks for consistency and continuity in the security provided and is it adequate to the task. E.g., does the SSL certificate Organization Unit field and Jurisdiction fields match the captured legal entity information. How does the policy and jurisdiction there relate to other beneficial entities. Importantly does this align with the policy expectations of the person.

TPI Metrics

Table 1: 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. T+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 to dynamic a measure of providing dynamic transparency in the context of ***once a technical session starts*** (which is at the time of collection), in context transparency over purpose and disclosures,
- -1 refers to where there is a provision of r analogue legal expectations, represented by legal requirements not specific to a digital context. E,g,
- -2 refers to the provision of low quality legally required information..
- -3 refers to the provision of non-operable transparency and digital privacy and related information.

Rating	**TPI1 - Timing (wrt to processing)**	**TP2**	**TPI3 Accessibility (trans performance)**	**TPI4 - digital security**
+1 (assured)	Before [Transparency of control/governance - Before, during or after processing]	+1 - credential is registered and present	Controller identity is presented prior to data collection - e	Security is required prior to collection (digital wallet based)
0 (dynamic assurance)	Just In time	0 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	is linked not presented	does not match you
- 3 (non-operative)	After	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.	is not valid or secure provider

404 Table 2: Transparency Performance Indicator Record Rating
405 Example

Field Name	**Field Description**	**Requirement: Must Shall May**	**TPI 1** before (out of band), just in time (before), at the start - or time of collection, during collection and after collection	**TPI 2** **Available** **Not Available**	**TPI 3** **Rate: +1, 0, -1, -2, -3,**	**TPI 4 Certificate or Key** **CN-Matches OU – Match Jurisdiction – Match (optional)**
Notice Location	Location the notice was read / observed	MUST	before, during, after	Present	+1	found
PII Controller Name	Name of presented organization	MUST		Present	0	Match
PII Controller Address	Physical organization Address	MUST		Present	0	Not match
Privacy Contact Point	Location / address of Contact Point	MUST		Present	1	Not match
Privacy Contact Method	Contact method for correspondence with PII Controller	MUST		Present	-1	No Match

Session key or Certificate	A certificate for monitored practice	MUST		Present (or Not-found)	1 (or –3)	Present (or No Security Detected)

406

407 Summary

408 In summary, Transparency Performance Indicators, TPIs are specified here for people
409 to use depending on context, location, security, and other out of session elements.
410 TPIs are digital transparency tool used to self determine how much a service context
411 can be trusted.

412 These TPIs are designed to work with open standards, the ANCR WG Royalty Free
413 license, which requires open source software license to be valid for conformance.
414 Transparency tools are required to be open in multiple ways for people to be able to
415 use and create records they can own and keep across and independently of service
416 providers.

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

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

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

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

427

428

APPENDIX A: TPI COMPLIANCE ASSESSMENT SCHEME PART 2

A.1 Operational Transparency Assessment

TPI – Operational Transparency Performance assurance test,

Most often, there is a missing, but required for operational digital governance, identifying attributes, held by commercial interest which systemically capture and control digital commons assets.

i) Transparency required to be available in context, during the time when PII is obtained (found in Transparency Statement or Privacy Policy [note]
   a. Period of time 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 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,
      i. Note: (Added by Editor) and who controls access to the authoritative version of the data processed.
   f. Existence of
      i. AI, or any Automated decision-making technology,
      ii. digital identity management surveillance technologies
      iii. any profiles generated
      iv. Meaningful information about the logic involved, [Note]
         1. its significance
         2. Expected consequences for and to Data subject

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. Demonstrating a non-performant form of data governance.

Conformity Assessment: utilizing the 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

1. TPI measuring the point when the individual is notified versus when personal information/digital identifiers are collected and processed. Capturing the timing of notice presentation in relation to first data capture

2. TPI 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 Controller identity and entity information and access point

3.TPI for how accessible the transparency is (transparency of digital transparency and the accessibility of the notice access for use

4.TPI validating the cybersecurity information versus the digital transparency information capturing the SSL certificate or keys and its associated meta-data.

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

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

Rating - Instruction	TPI 1 - Timing (wrt to processing)	TP2 - Required Info Presentation	TPI3 Accessibility (trans performance)	TPI4 - 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 automatically prior to session (out of band) in a machine-readable format. Number of ways 1. is a Controller Identity Trust registry 2. is 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	0 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, the assessment question would be	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)

480

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

482 In this appendix, here is a notice record template to fill out when recording a rating,
483 along with a rating template, and analysis results format.

484 Notice Record Schema & , Notice Record and Report - Template and Example

485

486

FIELD NAME	FIELD DESCRIPTION	REQUIREMENT: MUST, SHALL, MAY	FIELD DATA EXAMPLE
Notice Location	Location the notice was read/observed	MUST	Walmart.com | Save Money. Live Better
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
Privacy Contact Point	Location/address of Contact Point	MUST	Org.com/privacy.html
Session Certificate	A certificate for monitored practice	Optional	SSL Certificate Security (TLS) and Transparency

487

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 reference to Report on the Adequacy of Digital Identity Governance, for cross border transparency and consent.

PII Controller must:

1. Must 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/