Transparency Performance Indicators: PII Controller Identification for Valid Consent

A Kantara Initiative Recommendation

Version: 1.0

Document Date: 2025-05-21

Editors: Mark Lizar

Contributors: Gigliolla Agassini, Salvatore D'Agostino, Tim Lloyd, Tim Reiniger, Daniel Schleifer

Produced by: Anchored Notice and Consent Receipt Work Group (ANCR)

Status:

This document is a Draft Recommendation produced by the Anchored Notice and Consent Receipt Work Group (ANCR). The Group has approved it for Public Comment and Intellectual Property Rights Overview.KI-Group-Approved-DraftKI-Public-Review-DraftKI-Group-ApprovedKI-Kantara-Initiative-CandidateKI-Kantara-Initiative-Final-RecommendationKI-Kantara-Initiative-Final-Report See the Kantara Initiative Operating Procedures for more information.

Abstract:

Transparency Performance Indicators (TPIs) are a novel approach to digital trust transparency and consent reporting. TPIs clarify when notice and consent is valid for digital identification online. Here there are 4 TPIs for valid consent 1. the timing of the notice, 2. the content of the notice, 3. access and usefulness of the notice, and 4. authority and security. These measure risk of (hidden) identification, and tracking (surveillance) of the PII Principal. This represents a

significant advancement for decentralizing digital identification and surveillance governance with standard notice and consent records for proof of authority in online systems.

The TPIs measure transparency for valid consent in accordance with Convention 108+, the authoritative international commonwealth data governance framework for 58 countries and 2.5 billion people, in which transparency is required for security and privacy.

TPI Report for valid consent is developed in the Kantara Initiative Anchored Notice and Consent Receipt Work Group (ANCR) as an alternative to surveillance capitalism (without permission and consent.) of ubiquitous platforms while promoting open standards for security and privacy online.

IPR Option:

This document is subject to the Kantara Initiative IPR Policy Option: Reciprocal Royalty Free with Opt-out to Reasonable and Non-Discriminatory (RAND)

Any derivative use of this specification must not create any dependency that limits or restricts the open use, transparency, accessibility, or availability of the specification and/or its use to measure the performance of transparency and/or the ability for the PII Principal to receive a notice receipt, or to manage or present a notice receipt as a record of and for the authoritative use of PII Principal consent.

Suggested Citation:
Transparency Performance Indicators for the Assessment of Valid Consent V1.0. Kantara Initiative Anchor Notice and Consent Receipt Work Group. 2025-05-21. Kantara Initiative Recommendation. URL TBD UPON PUBLICATION

NOTICE AND CONDITIONS FOR USE

KI-IPR-RAND

KI-IPR-CCSA

-

License Condition:

This document has been prepared by participants of Kantara Initiative Inc. ANCR-WG. No rights are granted to prepare derivative works of this ANCR TPI measurement methodology outside of the ANCR WG. Entities seeking permission to reproduce this 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, express or implied, including any warranties of merchantability, non-infringement of third-party intellectual property rights, or fitness for a particular purpose. Implementers of this Transparency Performance Indicators specification are advised to review Kantara Initiative's website for information concerning any Necessary Claims Disclosure Notices that have been received by the Kantara Initiative Board of Directors.

DEAR READER

Thank you for reviewing this specification in its preparation for publication and contribution. Kantara Initiative is a global non-profit dedicated to improving the secure, private, and trustworthy use of digital identifier surveillance through innovation, standardization, and good practice.

Kantara is known around the world for incubating innovative concepts, operating Trust Frameworks to assure digital identification & privacy service providers, developing community-led best practices into specifications and standards. Its efforts are acknowledged by OECD ITAC, UNCITRAL, ISO SC27 JTC 1 WG 5, other consortia, and governments around the world. 'Join, Innovate, Trust' captures the rhythm of Kantara in an inclusive, equitable digital community offering value and benefit to all.

Every publication, in every domain, is capable of improvement. Kantara welcomes and values your contribution through membership, sponsorship, active invite to participate in the ANCR Work Group and the Kantara Initiative where its transparency and consent is reflected in the entire organization.

Table of Contents

Figures and Tables

(Appendices)

1. Introduction

The capacity to consent prioritizes and elevates the privacy principle of openness, and transparency to the first operational principle. Transparency, knowledge of whom one is providing permission to, with the legal authority of consent is critical. Openness is a fundamental democratic requirement, entrenched in legislation in all countries, cultures, and governing contexts, and a universal requirement for knowledge transfer. When any type of identification or recorded surveillance of individuals occurs, identification of the PII Controller, that is, who is doing the surveillance, is required unless legally specified otherwise. Trust in general, and of a PII Controller, in the protection and control of personal information, in both physical and online spaces, requires first transparency, of authority and the presentation of who is accountable.

Transparency is required for safety, security, and privacy in the use of digital identification technologies prior to collecting and processing personal data. This is a fundamental requirement for consent to be legally, technically, or socially possible.

These four (4) Transparency Performance Indicators (TPIs) measure 1. Timing of PII Controller Identification, 2. Presence of compulsory identification, 3. Security and privacy rights access, 4. Security and sovereignty. These are used to create a Transparency Performance Report (TPR) wherein a record of transparency is generated, and where performance is measured to determine if consent is valid and transparency operable.

The method presented here, produces a PII Controller notice identification record as evidence defined utilizing the ISO/IEC 29100:2024 Privacy framework, and the Kantara Consent Receipt v1.1, extending the privacy framework with in the now open and free to access ISO/IEC 27560:2024 TS Consent record information structure. These are applied here for a standard controller identification record of performance and demonstration of adequate transparency for consent.

Without a presentation of controller identification, there is no legal or technical way for people to be informed about who is in control and accountable for the security and privacy of online identification or the trustworthiness of “digital trust”). The PII Controller notice generated identification record, provides the means to map digital identity terms to traceable,accountable record , independent of service provided. Independent record of Controller identifiers is essential for trust, the security, and privacy, compulsory for consent, or any other legal basis regardless of justification, the type of identifier used, or who the Controller is.

Transparency modalities take the form of the timing and type of notice required to authorize organizations to collect, process, or otherwise identify an individual online, wherein a record of transparency is required to not only meet legal obligations, but to also scale the capacity to trust, actively monitor and enforce accountability and co-regulate the security and privacy for all stakeholders.

The audience for this transparency report is individuals,Controller organizations, social industry, developers, and data governance regulators. A TPI report supports stakeholders in observing a shared understanding of the active state of privacy through transparency performance. This is particularly relevant for the governance of identification in communications networks and information systems. By providing a standard Controller notice identification record specified to ISO/IEC 29100 privacy framework for recording and evaluating transparency for consent compliance internationally, fulfilling the TPI methodology and objective to assist stakeholders in navigating complex security and privacy considerations of utilizing consent for permitting cross border data flows, while fostering innovation in digital identification, its trusted transparency and compliance.

The TPI provides valid consent transparency to innovate transborder data security flow and validation for digital identification industry. It assesses whether transparency is operational and secure to validate consent.. The TPI methodology is a simple but effective compliance tool as it reports on Controller identification transparency rather than the Controller policy details, or technical implementation modalities of technology. Providing an operational method to measure the capacity for transparency in PII processing, and the validity of consent..

2. Scope

This document provides a methodology for observing, interpreting, and measuring the performance of PII controller identification transparency, providing a standardized structure for reporting and capturing evidence of (digital trust) and its compliance. The methodology is used to make a record to measure transparency performance to validate consent for digital identification and identifier based tracking and profiling of PII principals.

The transparency performance methodology for standards conformance provides standard evidence of the validity and legitimacy of consent for PII processing by utilizing Transparency Performance Indicators (TPIs).

TPI's capture of the PII Controller[1] required identification information by capturing the text of the first notification presented to generate a controller notice identification record. For example, for data processing on a website. Specifically, the four (4) TPIs measure: 1. Timing of PII Controller identification, 2. Presence of compulsory identification, 3. Security and privacy rights access, and 4. Security and sovereignty.

Legal compliance transparency is assessed in accordance with International Treaty Convention 108+, utilizing ISO/IEC JTC 1 WG 5 29100:2024 (Information technology — Security techniques — Privacy framework) which is interoperable to record the transparency modality in a PII controller notice identification record. A record of conformity assessment, which can then be used to measure the compliance to Convention 108+ conformant legislation . Interoperable with ISO/IEC 27001:2022 standard and framework. (Information security, cybersecurity and privacy protection — Information security management systems — Requirements). The PII Controller notice identification record generated with this methodology has many applications and can be

[1] The term controller is used with multiple adjectives in this document. One source of this is different terminology for a category of actor (see Appendix A. Table 1). Further, it is possible for the person to be subject, controller, and object granted. Another is the specific type of controller action taken. In the case of the PII Controller, here, the action measured is notice and so with it the specific role of the PII Controller as Notice Controller.

used for security and privacy benchmarking, generating notice and consent receipts, for withdrawal of consent, as evidence, for conformance, auditing compliance, and for transparency signaling.

3. Normative References

3.1 Council of Europe, Convention 108+ Convention for the Protection of Individuals with Regard to the Processing of Personal Data

1. An international Treaty expected to be fully ratified in 2025 to provide an authoritative international, and internet capable security and privacy framework.
2. Convention 108+ is ratified when 38 countries implement Adequate legislation
3. The Treaty, in particular transparency of processing, and notification requirements are,multi jurisdictional guidesis referenced in the appendix.
4. It provides an international validation for consent as a legal basis suitable for transborder data flows with common legal best practice.

3.2 ISO/IEC 29100:2024 Security and Privacy Technique

This standard is open and free to access "relates to PII in all ICT environments, specifying a common privacy terminology; defining the actors and their roles in processing PII; describing privacy safeguarding requirements; and referencing known privacy principles:

- Actors and roles
- Interactions
- Recognizing PII
- Privacy safeguarding requirements
- Privacy policies
- Privacy controls.
- Source bibliography

3.3 Kantara Initiative, Minimum Viable Consent Receipt, & Consent Receipt Specification

(published in ISO/IEC 29184:2020 Online privacy notice and consent appendix b) - providing a common transparency schema used to make the report.

Previously presented in support of Canadian meaningful consent regulation in 2017. https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/submissions-received-for-the-consultation-on-online-reputation/or/sub_or_15/

4. Terms & Definitions

The terms and their definitions used in this document adopt the terminology of the normative references. The following terms are introduced here.

PII Controller Identification Record

A record created with the information provided in the process of PII Controller Identification.

PII Controller notice Identification record

The record generated so as to provide proof of online controller identification notice. The compulsory Controller identification and access field and attributes, required to generate a record for proof of- notice and digital evidence of consent.

Editors Note: In the context of the GDPR, this is Data Controller identification record used as a credential, to generate a r generic Record of Controller Notice Activity or notice and consent receipt (in the ANCR WG

PII Controller notice Identification record Information

The compulsory Controller identification information, is\ required to be presented prior to processing of any Personally Identifiable Information (PII) physical address, contact information, and a privacy rights access point, in order to ensure transparency regarding the applicable policy jurisdiction and the legal authority governing the processing of personal data.

Notice Type

Used in this document to describe the type of notice that constitutes transparency, of Notice, Notification, Disclosure, Statement, as well as Policy, or information display, like a web browser security screen, or a WebPage, or physically, a Sign, or signal like a blinking light

Abbreviated terms

- AI – Artificial intelligence
- ANCR – Anchored Notice and Consent Receipt
- CAI - Commission d’accès à l’information (Quebec)
- CBOR – Concise Binary Object Representation

- CI – Controller Identification
- CoE – Council of Europe
- COSE – CBOR Object Signing and Encryption
- DIDs- Decentralized Identifiers
- EDPB -European Data Protection Board EEC – European Economic Community
- GDPR General Data Protection Regulation
- ISO/IEC – International Organization for Standardization/International Electrotechnical Commission
- JOSE – JavaScript Object Signing and Encryption
- mDL – Mobile Driver License
- PII – Personally Identifiable Information
- SSL – Secure Socket Layer
- SPAP – Security and Privacy Access Point
- TLS – Transport Layer Security
- TPI – Transparency Performance Indicator
- TPR – Transparency Performance Report(ing)

5. Methodology

The transparency modalities are captured, recorded, and measured using the PII Controller identification record (Appendix A). This records transparency performance, to measure if consent is valid, operational, and how secure, i.e., what the scope of identification disclosure is, for consent, using the 4 TPIs..

5.1 Transparency Performance Indicators (TPIs)

These four (4) Transparency Performance Indicators are specified to measure a transparency modality conformance for valid consent compliance, providing the PII principal insight into how meaningful and operationally adequate it is, for Convention 108+ , and ISO/IEC standard interoperable privacy framework.

Consent is permission for identification is provided before being identified. Valid online only if PII Controller identification is presented before data collection, partially valid when after data is collected but before processing like on a website, using IP addresses for example, and not valid if identification is provided after processing. Consent is measured as capable of being meaningful, if access to security and privacy is proportionate to data collection, scope of disclosure is localised and access to control disclosure is capable in the service context.

As indicated in figure 1, the Transparency Performance Indicators are applied in sequence and determine whether the legal basis of consent is valid, and technically whether PII Controllers have met the functional obligation of notice. The four (4) TPIs are:

1. *Timing of PII Controller identification:*
   This TPI captures the timing of PII Controller identification presentation. It requires an assessment of wether Controller Jurisdiction and identification was presented prior to collection, or processing PII.
2. *Presence of compulsory identification:*
   Records the extent to which the compulsory Controller identification attributes are provided (Present/Not Present)
3. *Security and privacy rights access:*
   Measures how accessible the required PII Controller identification and privacy access transparency is, from within the service session and online context. In addition, it measures

how performative the Controller security and privacy access point is, assessing how accurate, complete, and operational (i.e., usable) digital privacy access is in practice.

4. *Security and sovereignty:*

This indicator records the digital certificate(s), keys, and other tokens that may be employed to secure the technical interaction and or encrypt a session. It examines identification, location, jurisdiction, and governance sovereignty (source of authority) information from the first 3 TPIs compared with the technical security information recorded in this 4th TPI (the associated certificates, object identifiers, policy and associated endpoint if accessible), for a measure of risk for national security integrity. While this is further facilitated by network connectivity it is possible to provide some or all this information in the form of an offline document.

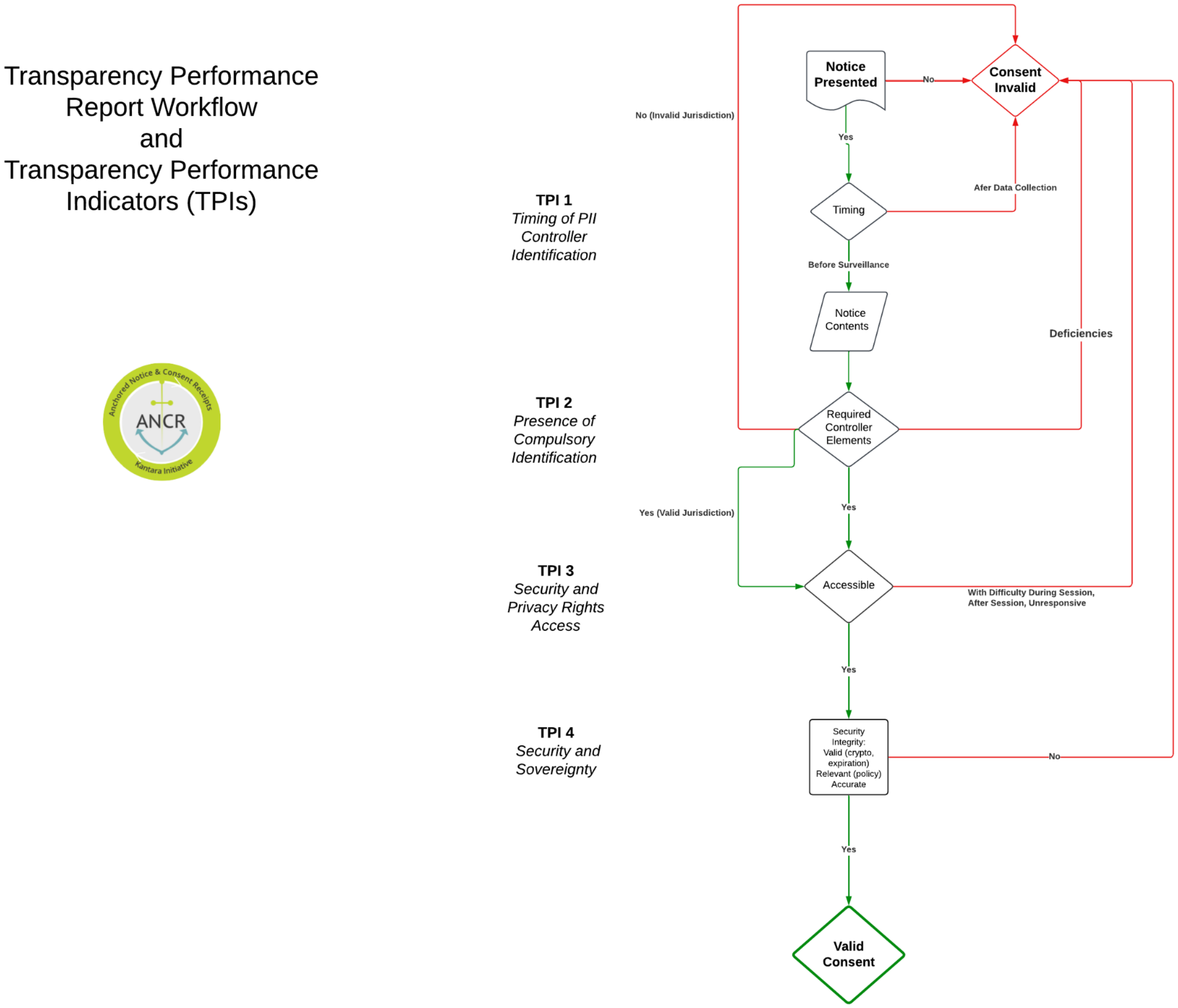
Transparency Performance Report Workflow and Transparency Performance Indicators (TPIs)
Anchored Notice & Consent Receipts
ANCR
Kantara Initiative
Notice Presented
No
Consent Invalid
No (Invalid Jurisdiction)
Yes
Afer Data Collection
TPI 1
Timing of PII Controller Identification
Timing
Before Surveillance
Notice Contents
Deficiencies
TPI 2
Presence of Compulsory Identification
Required Controller Elements
Yes
Yes (Valid Jurisdiction)
TPI 3
Security and Privacy Rights Access
Accessible
With Difficulty During Session, After Session, Unresponsive
Yes
TPI 4
Security and Sovereignty
Security Integrity: Valid (crypto, expiration) Relevant (policy) Accurate
No
Yes
Valid Consent

Figure 1. Transparency Reporting Workflow and Transparency Performance Indicators

5.2 Considerations

Only PII Controller notified identification and privacy access are measured, as these indicators assess the conformance and compliance that is globally required for valid consent, without having to map all the privacy laws in the world. . This does not assess services specific information, for example; service purpose, legitimacy of processing, authority to process PII (i.e., the grant of permission for processing), or a more granular scope of processing, beyond what is sovereign. It provides often missing requirements for digital identification, tracking, or surveillance based transparency and trust requirements.

In physical spaces, PII Controller identification, security, and rights access should, and in many cases, MUST be attached to surveillance signs, posted at the entry to physical space under surveillance, whether by a person or using digital technologies. In the case of online services, or on a device, all screens and user interfaces can be considered a notice, wherein PII Controller identification and privacy access is required to be and can be presented.

6. Transparency Performance Indicator Metrics, Analysis, and References

The Convention 108+, Treaty specifies transparency is required for “consent and all other legal purposes” to meet the requirements for adequacy. The convention itself is based on Fair Information Practice Principles where transparency over where and who Controllers are widely implemented even in non-commonwealth countries. As a result, Convention 108+ provides the authoritative privacy policy for adequacy with regards to global Internet and digital privacy. ISO/IEC 29100 is used here as the security framework interoperable with Convention 108+ implementations, like the GDPR which th extends the Convention 108+ as a regulatory framework, which is what defines what is required to be provided in the of, PIIController notice information record.

While the TPIs can be used to quickly self-assess transparency, its performance, capacity, and security, the methodology for generating PII Controller notice identification records requires that the technical environment is documented. y. In addition to the TPIs, this can include notice type, device type, operating system, software used for discovery (e.g. a web browser, or app, and version) or method for search identified. See Appendix A, Supplementary capture record.

6.1 TPI 1 – Measuring the Time of Controller Identification

The first Transparency Performance Indicator can be used by itself to self check if consent is valid at the point in time the first notice is presented and a digital relationship with Controller is technically created versus when PII is first generated and collected, as opposed to (versus) ***when shared*** PII is generated, stored and or processed. Tables 1, 2, and 3 below specify the information captured, how it is measured, recorded, and analysed to demonstrate compliance performance of transparency and its adequacy for commonwealth regulated jurisdictions.

Table 1. TPI 1 Measurement and Description

TPI 1 - Timing Measure	Description	Measure

Before collecting PII	Controller identification is presented before data is collected	+1
Before processing PII	Controller identification was provided before after PII was collected or generated, but before PII was processed	0

(table 1 continued on next page)

Table 1. TPI 1 Measurement and Description cont.

TPI 1 - Timing Measure	Description	Measure
After collection and processing of PII	Controller identification was provided after processing	-1

6.1.1 Analysis

Table 2. TPI 1 Analysis of Timing

Result	Analysis
+1	For valid consent, the controller identification MUST be presented prior to processing.
0	If the Controller, or Joint Controllers identification is presented after data is collected but before processed then consent is valid, only if the PII is not sensitive, and not collected in a sensitive context, not a minor or vulnerable person, is fair and not deceptive, or is pseudonymous, and is not disclosed, or shared directly without explicit permission with any

	unknown 3rd party PII controllers, or PII processor.
-1	If the Controller, or Joint Controller Identification is provided after collection and processing of PII then Consent is not valid.

Note: The measurement scale, 0 (low-risk consent/consensus) is for low-risk partial compliance and conforms to a decision by the European Data Protection Board (EPDB) on the 16th of January 2025. Pseudonymous data is a type of personal data according to the EDPB, “if the additional information needed to attribute it to an individual is held by someone else.” As a result, pseudonymized identifiers, or credentials, do not automatically become anonymous in the hands of a third party who does not have access to the additional information.

For valid, and meaningful consent, the individual must be informed of what pseudonymous information is generated or collected before it is processed by a 3rd Party Controller or transferred across borders. This is like showing live Video Surveillance on a screen at the entrance to a video recorded space.

6.1.2 Legal or Standard Reference for Timing of Controller Identification

Table 3. TPI 1 Legal and Standard References

Instrument	Reference	Text
Convention 108+	Recital 68, p.23	68. Certain essential information has to be compulsorily provided in a proactive manner by the controller to the data subjects when directly or indirectly (not through the data subject but through a third-party) collecting their data, subject to the possibility to provide for exceptions.
GDPR	Article 13.1 b), and 141, a) and b)	all data is obtained, provide the data subject with all the following information: (a) the identity and the contact details of the controller; (b) the contact details of the data protection officer. (Recital 42) Where processing is based on the data subject's consent, the controller should be

		able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC (1) a declaration of consent pre- formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(table 3 continued on next page)

Table 3. TPI 1 Legal and Standard References cont.

Instrument	Reference	Text
Q-Law 25, CAI Guidance	CAI (pg6) B.9. Timing of Consent	An organization must obtain consent before performing the actions to which it relates.
ISO/IEC 29100 Reference	6.2 Consent & Choice	Providing PII principals, before obtaining consent, with the information indicated by the openness, notice, and choice principle.

6.2 TPI 2 – Controller Identification Record Elements

This TPI captures the ‘required and compulsory controlled identification and access attributes into a PII Controller notice identification record (Appendix A). The following tables 4, 5, and 6 provide details on the identifiers captured, how they are measured, and the legal requirements and standards they are measured to demonstrate   compliance and adequacy with.

Table 4. TPI 2 Measurement and Description

TPI 2 - Compulsory Information Measure (CIM)	Description	Measure
All PII CIM Requirements	Is the compulsory identification information and access point information provided?	+1
Partial PII CIM Requirements	If the compulsory information is provided but the information to access it is not provided?	0
After collection and processing of PII CIM	Is the identification information provided non-existent or non-operable?	-1

6.2.1 Analysis of Compulsory Identification Attributes

These PII Controller identification elements MUST be provided by the PII Controller and are compulsory to enable operational personal data.[2]

Table 5. TPI 2 Analysis of Compulsory Information

Result	Analysis	Notes
+1	100% of the required attributes are presented	The required PII controller identification information for a record of processing activity that allows the external discovery of the controller, legal entity name, address, data sovereignty, including jurisdiction, and privacy access point.
0	90% ("most) of the controller information is provided and/or security and privacy rights	Partial digital transparency, can be compliant in physically secure and in person, or out of digitally recorded context for

[2] REGULATION EU General Data Protection (EU GDPR) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

	access point not provided.	explicit consent.
-1	Any listed controller identification information is missing.	----

449 ### 6.2.2 Legal & standards references for compulsory identification elements

450 *Table 6. TPI 2 Legal and Standards References*

Reference Controller identification	Reference	Quote
CoE 108 + (Code of Conduct)	Recital 68 p.23	Certain essential information has to be **compulsorily** provided in a proactive manner by the controller to the data subjects when directly or indirectly (not through the data subject but through a third-party) collecting their data, subject to the possibility to provide for exceptions in line with Article 11 paragraph 1. Information on the name and address of the controller Information on the name and address of the controller (or co-controllers), the legal basis and the purposes of the data processing, the categories of data processed and recipients, as well as the means of exercising the rights can be provided in any appropriate format (either through a website, technological tools on personal devices, etc.) as long as the information is fairly and effectively presented to the data subject. The information presented should be easily accessible, legible, understandable and adapted to the relevant data subjects (for example, in a child friendly language where necessary).
GDPR	Article 13.1, 14.1	(a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable;
Quebec Law 25/CAI Guidance	B.3 Consent and Collection	Comply with its **obligation of transparency** by providing accurate and complete information to the persons concerned when the collection is made from them4.
ISO/IEC 29100	5.6 pg.13	An external privacy policy provides outsiders to the organization with a notice of the organization's privacy practices, as well as other relevant information such as the identity and official address of the PII

	controller, contact points from which PII principals can obtain additional information, etc.The term “privacy policy” is used to refer to the internal privacy policy of an organization. External privacy policies are referred to as **notice, or notice, control and protection policies**.

6.2.3 PII Controller Record Conformance

The following PII Controller ‘identity’ requirements captured in the PII Controller identification process, is an explicit security presentation, and/or a privacy notice statement that can assessed in conformance to the ISO/IEC 29184:2020, or 27560:2024 TS or the Kantara Consent Receipt v1.1: All jurisdictions and records require this information to br provided,

1. Legal Entity Address
2. Legal jurisdiction(s) Controller Privacy Access point and Contact when applicable
3. The means for accessing privacy and transparency
4. Privacy policy or access point

6.3 TPI 3 – Security and Privacy Access

This TPI measures the accessibility of the Controller identification presentation and means for accessing rights. Tables 7, 8, and 9 below provide details on the information captured and how it is measured as well as the legal requirements and standards where this TPI shows compliance and adequacy.

Table 7. TPI 3 Measurement and Description

TPI 3 - Access Measure	Description	Measure
Access point presented with Controller identification presentation[3]	The security and privacy access point, is dynamically accessible and provided with Controller identification, including, data privacy officer contact	+1

[3] At no time is there a requirement for the identification or the creation of an identifier for the data subject/PII principal.

Access Point (scrolling page)	The security and privacy access point, is operational and easily accessed (out of context)	0

(table 7 continued on next page)

Table 7. TPI 3 Measurement and Description cont.

TPI 3 - Access Measure	Description	Measure
Access point analogue or buried (two links)	Data privacy access point is not easily accessed, is not operational	-1

6.3.1 Analysis of Access

This indicator also takes into account the additional Controller information and data collected for the TPI and includes device and user interaction, accessibility, language of presentation, and the number of "screens" that must be traversed to access and use privacy information to exercise the PII Principals rights.

Table 8. TPI 3 Analysis of Access

Accessibility of Access	Description	Measure
Dynamically accessible and meaningful, within the context.	Dynamic access to security and privacy can occur when for example the PII Principal can control and has access to their PII. The Controller identification is presented prior to data processing, and when access to privacy rights has a meaningful result.	+1
Operationally accessible, but not accessible in context, requires analog interactions.	Operational privacy access information can come in the form of contact information, that can be used in the context of the digital service but requires additional actions outside of the current user workflow.	0
Inoperable or accessible and not	Non-operable, refers to privacy access that is	-1

meaningful.	analogue, and out of context for example a mailing address, or when privacy access is not immediately accessible at the time of processing PII.

6.3.2 Legal References for Accessibility of security and privacy rights access

Table 9. TPI 3 Legal and Standards References

Instrument	Reference	Text
CoE Convention 108 +		“Article 8 - Transparency of processing 68. can be provided in any appropriate format (either through a website, technological tools on personal devices, etc.) as long as the information is fairly and effectively presented to the data subject. The information presented should be easily accessible, legible, understandable, and adapted to the relevant data subjects (for example, in a child friendly language where necessary). Any additional information that is necessary to ensure fair data processing.”
GDPR	13.1 (b), 14.1 (b)	rights access
Quebec Law 25/CAI Guidance	B.2 Methods of Control a)	Through rights (access, rectification, etc.) or remedies (complaint to an organization or the CAI, etc.). To ensure that individuals can exercise these rights in full knowledge of the facts, the laws provide for **transparency** obligations for organizations;
ISO/IEC 29100	6.9 Individual participation and access (pg.17)	Adhering to the individual participation and access principle means: - giving PII principals the ability to access and review their PII, provided their identity is first authenticated with an appropriate level of assurance and such access is not prohibited by applicable law;

6.4 TPI 4 – A measure of security information integrity

This TPI captures the relevant digital certificate(s), (e.g. x.509), or security token(s), e.g., (JavaScript Object Signing and Encryption (JOSE) or Concise Binary Objection Representation (CBOR) Object Signing and Encryption(COSE), and/or verifiable credential or mobile driver license documents (i.e., Decentralized Identifiers (DIDs) v1.0 or mDL) and keys to compare the public security meta-data, and policy objects against the required information in TPI 2. It checks for consistency and continuity in the security provided and is adequate. Tables 10, 11, and 12 below provide details on the information captured and how it is measured as well as the legal requirements and standards where this TPI shows compliance and adequacy.

Table 10. TPI 4 Measurement and Description

TPI 4 - Security and Sovereignty	Description	Measure
Transparent Security and Sovereignty	Transparency over extra-territorial data transfer sovereignty + security certificate or token identification matches Controller identification	+1
Transparent Security	Location does not cover local or regional distinction but does match at national or commonwealth level.	0
Non-Transparent, non-matching, or unknown Controller Security information	Location of processing and data subject not the same.	-1

6.4.1 Analysis

Table 11. TPI 4 Analysis of Security and Sovereignty

Result	Analysis	Measure
Dynamic	The TLS certificate Organization Unit and Jurisdiction fields match the captured legal entity information, extra-territorial data transfers are presented, and policy is appropriate for protection of PII.	+1
Operational	The TLS/SSL certificate OU matches and is in the same jurisdiction, or different jurisdiction, with some other security notification for extra-territorial data transfer	0
Not Operable	The TLS certificate OU does not match, or the legal jurisdiction is not sovereign to the PII Principal, no security information for data transfers. Object identifiers are not relevant in context.	-1

Note: Further checks can be done related to the cryptographic integrity of the keys and certificates, e.g. is TLS 1.3 being used, is the cipher suite adherent to the specification and related standards. The same can be done with other credential types and public keys.

6.4.2 Legal and Standards References

Table 12. TPI 4 Legal and Standards References

Instrument	Reference	Text
CoE 108 + (Code of Conduct)	Article 7 - Data Security 63 p.22 & 110. pg. 28	63. Security measures should take into account the current state of the art of data-security methods and techniques in the field of data processing. Their cost should be commensurate with the seriousness and probability of the potential risks. Security measures should be kept under review and updated where necessary. 110. The level of protection should be assessed for each transfer or category of transfers. Various elements of the transfer should be examined such as: the type of data; the purposes and duration of processing for which the data are transferred; the respect of the rule of law by the country of final destination; the general and sectoral legal rules applicable in the State or organization in question; and the professional and security rules which apply there.
GDPR	Recital 39	… Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorized access to or use of personal data and the equipment used for the processing.

(table 12 continued on next page)

504 *Table 12. TPI 4 Legal and Standard References cont.*

Instrument	Reference	Text
Quebec Law 25/CAI Guidance	Law 25 - 110 s12. (3)| Law 25 – 144 “(6) the other measures taken to ensure the confidentiality and security of personal information in accordance with this Act.”; Law 25 v- 159(4) does not take the security measures necessary to ensure the protection of the personal information in accordance with section 10;	if its use is necessary for the purpose of preventing and detecting fraud or of assessing and improving protection and security measures;
ISO/IEC 29100	6.11 Information security Adhering to the information security principle means:	Implementing controls in proportion to the likelihood and severity of the potential consequences, the sensitivity of the PII, the number of PII principals that might be affected, and the context in which it is held; - limiting

505

7. Summary

The ANCR WG recommends a method to assess the security, sovereignty and governance of consent in digital identification systems. It introduces Transparency Performance Indicators (TPIs) as a methodology to generate a report on the active state of transparency for valid consent. The associated PII Controller notification record can be further used, independently, to manage, including withdrawing, permission to process identification information with the authority and justification of valid consent. A TPI report is a valuable building block for record and receipt based governance and for reuse by the PII Principal as a PII Controller transparency notice record receipt.

This version 1.0 report is the first step; we look forward to its continuing evolution.

8. Appendix A: PII Controller Identification Record

Table A. 1 PII Controller Identification Record Fields

Field #	Controller ID Object	String	controller_id_object	_	Required
1	Capture presentation of PII Controller Identity \	text	presented_name_of_service_provider	name of service. E.g. Microsoft	May
2	PII Controller Identity & Contact	object	[piiController_identity]		
3	PII Controller Name	String	piiController_name	Company / organization name	MUST
	PII Controller address	String	piiController_address	_	MUST
4	PII Controller contact email	Varchar(n)	piiController_contact_email	correspondence email	MUST
6	PII Controller Phone	Char	piiController_phone	The general correspondence phone number	SHOULD
7	PII Controller Website	Varchar	piiController_www	URL of website (or link to controller application)	MUST

(table A.1 continued on next page)

Table A.1 PII Controller Identification Record Fields cont.

Field #	Controller ID Object	String	controller_id_object	_	Required
8	PII Controller Certificate	Blob	piiController_sslcertificate	A capture Website SSL	MUST
	means of accessing privacy rights and controls	VarChar(max)	pcpL	The end point address for privacy information and service access	MUST
9	Service Privacy Access Point (SPAP)-Other	string	pcp_other	Other	**
10	Privacy Contact Point Types (pcpT)	Object		pcpType	
	SPAP-MailAddress	object		Mailing address	MUST
	SPAP-Profile	String	pcpProfile	Privacy Access Point Profile	**
	SPAP-InPerson	String	pcpInperson	In-person access to privacy contact	**

(table A.1 continued on next page)

529 *Table A.1 PII Controller Identification Record Fields cont.*

Field #	Controller ID Object	String	controller_id_object	_	Required
10 *cont.*	SPAP-Email	Varchar	pcpEmail	PAP email	**
	SPAP-Phone	char	pcpPhone	Privacy access phone	**
	SPAP -PIP- URI	Varchar	pcpPip_uri	privacy info access point, URI	**
	SPAP-Form	Varchar	pcpForm	Privacy access form URI	**
	SPAP-Bot	String	pcpBot	privacy bot, URI	**
	SPAP-CoP	String	pcpCop-loc	Code of practice certificate, URI of public directory with pub-key	**
11	SPAP-Other	string	pcp_other	Other	**
	SPAP Policy link, notice, statement, label	text	pcpn/	the means of privacy	MUST

530

9. Appendix B: Role Mapping To Privacy and Security Instruments

ISO/IEC 29100 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).

Table B.1 Role Mapping

Stakeholder	ISO/IEC 29100	Conv 108+	GDPR	PIPEDA	Quebec Law 25[1]
Regulator	Privacy Supervising Authority	Supervisory Authority	Data Protection Authority	Privacy Commissioner	Commission d'accès à l'information du Québec
Principal	PII Principal	Data Subject	Data Subject	Individual	Concerned Person (or person concerned)
Controller	PII Controller	Data Controller	Data Controller	Organisation	Person in Charge of the Protection of Personal Information
Joint (or Co-) Controller	Joint PII Controller	Joint Data Controller	Joint-Controller	Organisations	Person in Charge of the Protection of Personal Information
Processor	PII Processor	Processor	Data Processor	3rd Party	Service Provider (prestataire de services)

(table B.1 continued on next page)

Table B.1 Role Mapping cont.

Stakeholder	ISO/IEC 29100	Conv 108+	GDPR	PIPEDA	Quebec Law 25[1]
Sub-Processor	Sub-Processor	Sub-Contractor	Sub-Processor	3rd Party / Service Provider	Service Provider (prestataire de services)
3rd Party	Any entity or individual other than the Data Subject, Controller or Processor	Any entity or individual other than the Data Subject, Controller or Processor	Any entity or individual other than the Data Subject, Controller or Processor	3rd Party	Any individual or organisation other than the person concerned or the organization in charge of data protection

Note: Quebec, Bill 64 - [1] An Act to modernize legislative provisions as regards the protection of personal information, SQ 2021, c 25, has compliance roles, mapped to be interoperable within data privacy frameworks.

Note: Roles in this document refer to a record of relationship between the Individual and a PII controller in the context of an identification based service, as documented by the Controller notice identification schema used in TPI assessments.

10. ISO/IEC 29100 Terminology Bibliography

[1] ISO Guide 733, Risk management — Vocabulary

[2] ISO 31000, Risk management — Guidelines

[3] SC 27 committee document 502 — Privacy References List, available at: https://committee.iso .org/home/jtc1sc27

[4] ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary

[5] ISO/IEC 27001, Information security, cybersecurity and privacy protection — Information security management systems — Requirements

[6] ISO/IEC 27002, Information security, cybersecurity and privacy protection — Information security controls

[7] ISO/IEC 27003, Information technology — Security techniques — Information security management systems — Guidance

[8] ISO/IEC 27004, Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation

[9] ISO/IEC 27005, Information security, cybersecurity and privacy protection — Guidance on managing information security risks

[10] ISO/IEC 27006, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

[11] ISO/IEC 27007, Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

[12] ISO/IEC TS 27008, Information technology — Security techniques — Guidelines for the assessment of information security controls

[13] ISO/IEC 270094), Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements

[14] ISO/IEC 27010, Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications

[15] ISO/IEC 27011, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations

[16] ISO/IEC 27013, Information security, cybersecurity, and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

[17] ISO/IEC 27014, Information security, cybersecurity, and privacy protection — Governance of information security

[18] ISO/IEC TR 27016, Information technology — Security techniques — Information security management — Organizational economics

[19] ISO/IEC 27017, Information technology — Security techniques

[20] ISO/IEC 29100:2024 Information technology – Security techniques - Privacy Framework