

# Transparency Performance Indicators

## A Benchmark for Valid Controller Identification & Consent

### A Kantara Initiative Recommendation

**Version:** 1.0

**Document Date:** 2025-02-12

**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. See the Kantara Initiative [Operating Procedures](#) for more information.

**Abstract:**

Transparency Performance Reporting (TPR) is a novel approach to digital transparency and data control reporting. TPR clarifies when a notice and consent receipt is required and its validity and provides a litmus test for valid consent. TPR uses 4 transparency performance indicators (TPIs) – the timing of the notice, the content of the notice, access and usefulness of the notice, and sovereignty of authority and security – to measure the transparency of the Personally Identifiable Information (PII) Controller notice of risk to the personal data of the PII Principal. This represents a significant advancement for decentralizing digital identification and data surveillance governance within data flows.

TPR includes mapping to privacy frameworks including Convention 108+, a commonwealth data governance framework that covers 2.5 billion people, and with it an interoperable set of

# Transparency Performance Reporting

---

requirements for security and privacy. The mappings show how the TPIs address the requirements for records of processing activities (GDPR Article 30), enable services to be accountable to international (internet) standards for data governance, and create a technical record foundation in a common set of rules allowing people to have their authoritative records of digital identification relationships.

TPR was developed through volunteer work over three years in the [Kantara Initiative Anchored Notice and Consent Receipt Work Group \(ANCR\)](#) as a means of understanding and addressing ubiquitous platform and application surveillance while promoting open security and privacy legal standards.

## **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 Reporting for the Assessment of Digital Identification Surveillance V1.0.* Kantara Initiative Anchor Notice and Consent Receipt Work Group. 2025-02-12. Kantara Initiative Recommendation. URL TBD UPON PUBLICATION

# Transparency Performance Reporting

---

## NOTICE AND CONDITIONS FOR USE

Copyright: The content of this document is copyright of Kantara Initiative, Inc.  
© 2025 Kantara Initiative, Inc.

### 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 Scheme 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 identity & 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. 'Join, Innovate, Trust' 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, active participation in the [Work Group](#)*

---

Document Version: 1.0

Document Date: 2025-02-12

## Transparency Performance Reporting

---

95 *that produced this, and participation in all our endeavors so that Kantara can reflect its value to*  
96 *you and your organization.*

# Transparency Performance Reporting

---

97	<b>Table of Contents</b>	
98	<b>1. INTRODUCTION .....</b>	<b>7</b>
99	<b>2. SCOPE .....</b>	<b>9</b>
100	<b>3. NORMATIVE REFERENCES .....</b>	<b>11</b>
101	3.1 CONVENTION 108+ CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA	11
102	3.2 ISO/IEC 29100:2024 SECURITY AND PRIVACY TECHNIQUE.....	11
103	3.3 KANTARA INITIATIVE, MINIMUM VIABLE CONSENT RECEIPT, & CONSENT RECEIPT SPECIFICATION .....	11
104	<b>4. TERMS &amp; DEFINITIONS.....</b>	<b>12</b>
105	<b>5. METHODOLOGY .....</b>	<b>14</b>
106	5.1 TRANSPARENCY PERFORMANCE INDICATORS (TPIs) .....	14
107	5.2 CONSIDERATIONS .....	16
108	<b>6. TRANSPARENCY PERFORMANCE INDICATOR METRICS, ANALYSIS,.....</b>	<b>17</b>
109	6.1 TPI 1 – MEASURING THE TIME OF CONTROLLER IDENTIFICATION .....	17
110	6.2 TPI 2 – CONTROLLER IDENTIFICATION RECORD ELEMENTS.....	20
111	6.3 TPI 3 – SECURITY AND PRIVACY ACCESS.....	23
112	6.4 TPI 4 – A MEASURE OF SECURITY INFORMATION INTEGRITY .....	26
113	<b>7. SUMMARY .....</b>	<b>30</b>
114	<b>8. APPENDIX A: PII CONTROLLER IDENTIFICATION RECORD .....</b>	<b>31</b>
115	<b>9. APPENDIX B: ROLE MAPPING ACROSS PRIVACY AND SECURITY INSTRUMENTS.....</b>	<b>34</b>
116	<b>10. ISO/IEC 29100 TERMINOLOGY BIBLIOGRAPHY .....</b>	<b>36</b>
117		
118		
119		
120		

# Transparency Performance Reporting

---

121	<b>Figures and Tables</b>	
122	Figure 1. Transparency Reporting Workflow and Transparency Performance Indicators .....	15
123		
124	Table 1. TPI 1 Measurement and Description .....	17
125	Table 2. TPI 1 Analysis of Timing.....	18
126	Table 3. TPI 1 Legal and Standard References .....	19
127	Table 4. TPI 2 Measurement and Description .....	20
128	Table 5. TPI 2 Analysis of Compulsory Information .....	21
129	Table 6. TPI 2 Legal and Standards References .....	22
130	Table 7. TPI 3 Measurement and Description .....	23
131	Table 8. TPI 3 Analysis of Access.....	24
132	Table 9. TPI 3 Legal and Standards References .....	25
133	Table 10. TPI 4 Measurement and Description .....	26
134	Table 11. TPI 4 Analysis of Security and Sovereignty .....	27
135	Table 12. TPI 4 Legal and Standards References .....	28
136		
137	<i>(Appendices)</i>	
138	Table A. 1 PII Controller Identification Record Fields .....	31
139		
140	Table B.1 Role Mapping.....	34
141		

## 1. Introduction

---

The capacity to consent is underpinned by the privacy principle of openness, and knowledge of to whom one consents is critical. Openness is a fundamental democratic requirement, entrenched in legislation in all countries, cultures, and governing contexts. When any type of identification or recorded surveillance of individuals occurs, identification of who the PII Controller is, that is, who is doing the surveillance, must be presented. Trust, in the protection and control of personal information, in both physical and online spaces, requires the presentation and the identification of who is accountable.

For safety, security, and privacy in digital identification technologies, transparency is required for inclusive identification and required prior to collecting and processing personal data. This is a foundational requirement for consent to be legally, technically, or ethically possible. This transparency is the focus and goal of this document.

This Kantara Initiative recommendation specifies four (4) Transparency Performance Indicators (TPIs) that indicate if Consent is valid for any surveillance context: 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 operable.

The resulting PII Controller identification record is evidential as it is defined here with ISO/IEC 29100:2024 Privacy framework, using the Kantara Consent Receipt v1.1, which has evolved now into the ISO/IEC 27560:2024 Consent record information structure. It is applied here to enable the measure of international (internet) legal adequacy, of transparency for consent. This represents, and is required as, the underlying legal justification for digital identification management technologies.

# Transparency Performance Reporting

---

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, privacy, and sovereignty of surveillance in short how trustworthy is “digital trust”). Without the PII Controller identification record, there is no traceability or accountability for misinformation, independent of service providers, much like running a business without auditing or accounting with generally accepted principles. This requirement is essential for human security, compulsory for consent, or any type of legitimate processing regardless of justification or the Controller.

Transparency modalities take the form of the timing and type of notice required to authorize organizations to collect, process, or otherwise surveil an individual, transparency is required to not only meet legal obligations, but also for the capacity to trust and enforce accountability for all security and privacy stakeholders.

The audience for this transparency report is individuals, organizations, developers, and regulators. This report's objective is to support these stakeholders in observing the active state of transparency and its performance. This is particularly relevant for the governance of surveillance in communications networks and information systems. By providing a structured framework for recording and evaluating transparency, the TPR's objective is to assist stakeholders in navigating complex security and privacy considerations while fostering innovation in digital trust transparency and its legal compliance.

The TPR provides a minimum consent and sovereign security validation tool for digital surveillance, identification, and artificial intelligence (AI) technologies. It assesses whether transparency is operational and secure as a prerequisite for consent. It has an extensive scope of application and can be extended into an international and inclusive benchmark. The TPR reports on Controller identification transparency rather than the technical details, or implementation mechanisms of technology. The specifics depend on various contextual factors beyond the scope of this report framework. Instead, the TPR provides a foundational approach to measuring transparency in PII processing, which can be extended in context by regulatory requirements.



## 2. Scope

---

This document specifies 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) compliance. It records and indicates how transparent digital identification surveillance is for humans.

This report provides evidence of the validity and legitimacy of consent for PII processing utilizing Transparency Performance Indicators (TPIs). TPI's capture of the PII Controller<sup>1</sup> required, security, privacy information focusing on capturing the first notification online independently of the PII controller to generate a controller 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. Together, they capture the state of operational capacity for transparency with respect to conformance and compliance.

Legal transparency can be measured against international Convention 108+ Privacy Treaty, utilizing the ISO/IEC JTC 1 WG 5 29100:2024 (Information technology — Security techniques — Privacy framework) and associated standard to record the transparency modality by creating a PII controller record. A record which can measure the performance of legislated law and or practice against the international Treaty. Also referred to as the global privacy policy framework, Convention 108+. The controller record, along with ISO/IEC 29100:2024, is also interoperable with ISO/IEC 27001:2022 standard and framework. (Information security, cybersecurity and privacy protection — Information security management systems — Requirements). The PII Controller identification and access record generated with this methodology has many

---

<sup>1</sup> 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.

## Transparency Performance Reporting

---

226 applications and can be used for security and privacy benchmarking, as evidence, for  
227 conformance, in auditing compliance, and for transparency signaling.  
228

## 3. Normative References

---

### 3.1 [Convention 108+](#) Convention for the Protection of Individuals with Regard to the Processing of Personal Data

1. Council of Europe, Convention 108+, an international treaty expected to be fully ratified in 2025, provides a formal global security and privacy framework.
2. It provides the standard instructions and requirements for the signatory countries to implement adequate interoperable privacy law and/or privacy law.
3. The treaty, in particular transparency of processing, and notification requirements, guides and provides the logic of the performance report and its measures as referenced in the appendix.
4. It provides an international measure of 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/](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 notice

The record generated so as to provide proof of notice. The minimum 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 generic Record of Controller Notice Activity or notice and consent receipt (in the ANCR WG*

### PII Controller Identification record notice 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.

### PII Controller Identification Record

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

### 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

# Transparency Performance Reporting

---

- 289 • COSE – CBOR Object Signing and Encryption
- 290 • DIDs- Decentralized Identifiers
- 291 • EDPB -European Data Protection Board EEC – European Economic Community
- 292 • GDPR General Data Protection Regulation
- 293 • ISO/IEC – International Organization for Standardization/International Electrotechnical
- 294 Commission
- 295 • JOSE – JavaScript Object Signing and Encryption
- 296 • mDL – Mobile Driver License
- 297 • PII – Personally Identifiable Information
- 298 • SSL – Secure Sockey Layer
- 299 • SPAP – Security and Privacy Access Point
- 300 • TLS – Transport Layer Security
- 301 • TPI – Transparency Performance Indicator
- 302 • TPR – Transparency Performance Report(ing)
- 303
- 304

## 5. Methodology

---

The transparency modality is captured, recorded, and measured using the PII Controller identification record (Appendix A). This records transparency performance, to assess if transparency is valid, operable, and secure, i.e., sufficient, for consent, using the 4 TPIs, or as otherwise justified, as in the case of non-consent-based surveillance.

### 5.1 Transparency Performance Indicators (TPIs)

These four (4) Transparency Performance Indicators are very specifically articulated to measure a transparency modality for valid consent, how meaningful it is, and operationally capable, to assess conformance with international (Internet suitable) Convention 108+, standard global privacy framework.

Consent is Valid if PII Controller identification is provided before data collection, partially valid if before processing with for example low risk pseudonymous identifiers, 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, sovereign and access capability.

As indicated in figure 1, the Transparency Performance Indicators conducted in sequence and can be used to determine whether there is a basis for valid consent, and more generally whether PII Controllers have met their obligations for notice. The four (4) TPIs are:

#### 1. *Timing of PII Controller identification:*

Captures the timing of controller identification presentation. It assesses if identification was provided prior to collection, before, or after 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 above compulsory controller identification information is in the service session context. In addition, it measures how accessible the Controller security and privacy access point is, and assesses how accurate, complete, and operational (i.e., usable) this information is in practice.

# Transparency Performance Reporting

## 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 sovereign 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.

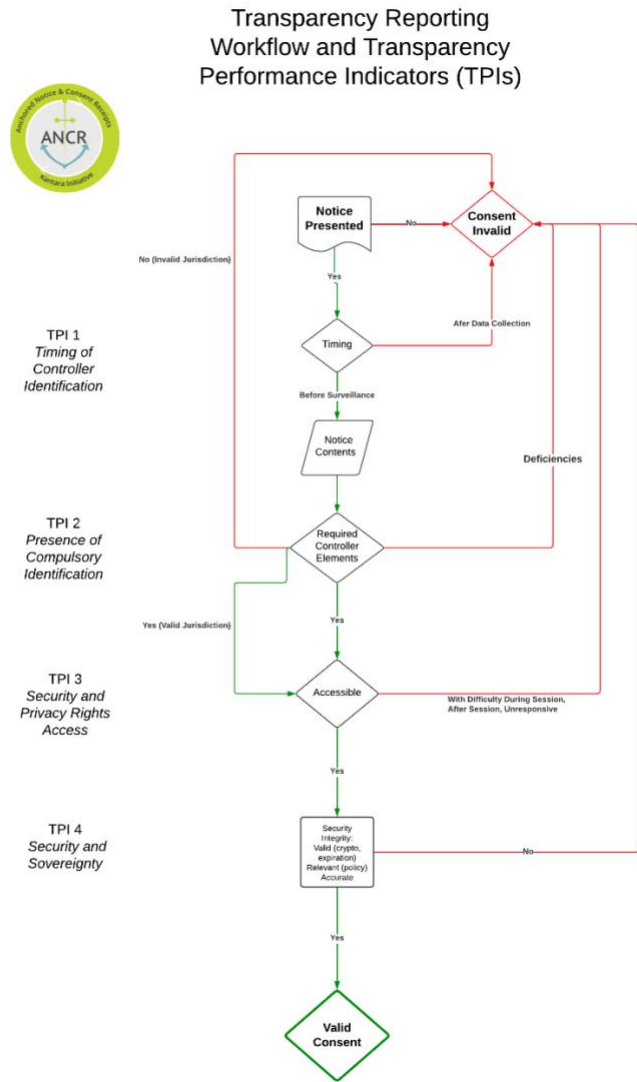


Figure 1. Transparency Reporting Workflow and Transparency Performance Indicators

## 5.2 Considerations

Only identification and access are measured, as these indicators assess the conformance and compliance that is globally required for surveillance, and authentic (i.e., from a legitimate authority) security, and privacy. This does not assess services specific information, for example; 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, referred to here and also known as surveillance trust (consented surveillance) 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 physically, whether by a person or using digital technologies, surveilled and secured spaces. In the case of online services, or on a device, all screens and user interfaces can be considered a notice, wherein Controller identification is required to be and can be presented.



6. Transparency Performance Indicator Metrics, Analysis, and References

The primary authoritative reference is Convention 108+, as this treaty specifies the requirements for adequacy which countries implement as legislation that can be enforced to ratify the Convention. The convention itself is based on principles widely implemented even in non-commonwealth countries. As a result, Convention 108+ is the authoritative privacy policy for adequacy with regards to global Internet and digital privacy. It is used here to extend the use of ISO/IEC 29100, which is used to specify and record the Controller information.

While the TPIs can be used to quickly self-assess transparency, its performance, capacity, and security, the methodology requires that the technical environment should be captured for evidential quality. In addition to the TPIs, the notice type, device type, operating system, discovery software (e.g. a web browser, or app, and version), and any search tool can also be identified. See Appendix A, Supplementary capture record.

6.1 TPI 1 – Measuring the Time of Controller Identification

This TPI captures the point in time the notice was presented versus when PII is collected, and **when** PII is processed. Tables 1, 2, and 3 below provide details on the information captured, how it is measured, and the legal requirements and standards where this TPI shows compliance and adequacy.

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 collected data was processed	0

(table 1 continued on next page)

# Transparency Performance Reporting

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 with an unknown 3rd party PII controller, or 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 (EDPB) 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.

# Transparency Performance Reporting

For valid, and meaningful consent, the individual must be informed of what pseudonymous information was collected before it is processed. This is like showing live Video Surveillance on a screen at the point of surveillance.

## 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)	<p>all data is obtained, provide the data subject with all the following information:</p> <p>(a) the identity and the contact details of the controller; (b) the contact details of the data protection officer.</p> <p>(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.</p>

(table 3 continued on next page)

# Transparency Performance Reporting

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 ‘compulsory controlled identification and access attributes into a PII Controller identification record (Appendix A). The following tables 4, 5, and 6 provide details on the information captured, how it is measured, and the legal requirements and standards where this TPI shows compliance and adequacy.

Table 4. TPI 2 Measurement and Description

TPI 2 - Compulsory Information Measure	Description	Measure
All PII CI Requirements	Is the compulsory identification information and access point information provided?	+1
Partial PII CI Requirements	If the compulsory information is provided but the information to access it is not provided?	0
After collection and processing of PII CI	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, although advanced and dynamic access, using existing records or receipts that might also meet the requirements of functional compliance.

# Transparency Performance Reporting

414 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 access point not provided.	Partial digital transparency, can be compliant in physically secure and in person, or out of digitally recorded context for explicit consent.
-1	Any listed controller identification information is missing.	----

415

416

# Transparency Performance Reporting

## 6.2.2 Legal & standards references for compulsory identification elements

Table 6. TPI 2 Legal and Standards References

Reference Controller identification	Reference	Quote
CoE 108 + (Code of Conduct)	Recital 68 p.23	Information on the name and address of the controller – the right of everyone not to be subject to a purely automated decision significantly affecting them without having their views taken into consideration (littera a.); – the right of everyone to request confirmation of a processing of data relating to them and (or co-controllers), the legal basis and the purposes of the data processing, the categories of data processed to access the data at reasonable intervals and without excessive delay or expense (littera b.); and recipients, as well as the means of exercising the – the right of everyone to be provided, on rights can be provided in any appropriate format
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 <b>obligation of transparency</b> by providing accurate and complete information to the persons concerned when the collection is made from them <sup>4</sup> .
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. In the context of this framework, the term "privacy policy" is used to refer to the internal privacy policy of an organization. External privacy policies are referred to as <b>notices</b> .

## 6.2.3 PII Controller Record Conformance

The following PII Controller ‘identity’ requirements captured in the PII Controller identification process and related record, is an explicit security presentation, and/or a privacy notice statement and can be used in the ISO/IEC 29184:2020, or 27560:2024, or the Kantara Consent Receipt v1.1 Controller identity and consent record and format:

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

Note: Record, attributes, and format have been widely implemented in the industry, to include Legal Entity (or natural person) Name and/or trading name.

## 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 <sup>2</sup>	The security and privacy access point, is dynamically accessible and provided with Controller identification, including, data privacy officer contact	+1
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)

<sup>2</sup> At no time is there a requirement for the identification or the creation of an identifier for the data subject/PII principal.

# Transparency Performance Reporting

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 meaningful.	Non-operable, refers to privacy access that is analogue, and out of context for example a mailing address, or when privacy access is not immediately accessible at the time of processing PII.	-1



# Transparency Performance Reporting

## 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 <b>transparency</b> 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 Object 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

# Transparency Performance Reporting

## 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	<p>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.</p> <p>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.</p>
GDPR	Recital 39	<p>... 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.</p>

(table 12 continued on next page)

# Transparency Performance Reporting

473 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

474

## 7. Summary

---

This ANCR WG Recommendation provides a method to assess the sovereignty and governance of digital identification systems, for valid consent in 4 ways, with key metric indicators to signify compliance. It introduces a Transparency Performance Indicators (TPIs) methodology to generate a report on the state of transparency. It can be further used, independently, to control identification data with the application of privacy rights. The report generated can be reused by the PII Principal, as a PII Controller transparency record, and sent back to the Controller, to establish a common state of understanding of data governance, and access to digital identity privacy rights. The recommendation's objective is to establish with this report, particularly the use of TPIs to provide a standard method of recording digital transparency, critical to governance and its enforcement.

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)

# Transparency Performance Reporting

496 Table A.1 PII Controller Identification Record Fields cont.

Field #	Controller ID Object	String	controller_id_object	_	Required
8	PII Controller Certificate	Blob	piiController_ssl certificate	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)



# Transparency Performance Reporting

500 Table A.1 PII Controller Identification Record Fields cont.

Field #	Controller ID Object	String	controller_id_object	_	Required
10	SPAP-Email	Varchar	pcpEmail	PAP email	**
cont.	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	**
	SPAP-Other	string	pcp_other	Other	**
	SPAP Policy link, notice, statement, label	text	pcpn/	the means of privacy	MUST

501

9. Appendix B: Role Mapping Across 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 <sup>[1]</sup>
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	3 <sup>rd</sup> Party	Service Provider (prestataire de services)

(table B.1 continued on next page)

# Transparency Performance Reporting

511 *Table B.1 Role Mapping cont.*

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

512  
 513 Note: Quebec, Bill 64 - <sup>[1]</sup> An Act to modernize legislative provisions as regards the protection of  
 514 personal information, SQ 2021, c 25, has compliance roles, mapped to be interoperable  
 515 within data privacy frameworks.

516 Note: Roles in this document refer to a record of relationship between the Individual and any  
 517 digital service, as documented by the Controller identification notice record and schema for  
 518 TPI assessment. (see [ANCR Wiki](#))

519

## 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