



1 **ANCR Digital Transparency Performance** 2 **Scheme: Parts 1 and 2**

3 *Conformity & Compliance Assessment v0.9.9*

4
5 *ANCR refers to an Anchored Notice & Consent Receipt, it is a record that is generated using*
6 *the Transparency Performance Indicator assessment, which provides a standard measure*
7 *of operational performance of the present PII Controller's security and privacy session*
8 *information.*

9
10 Editor(s):

- 11 • Mark Lizar, WG Editor

12 Contributors:

- 13 • Sal D'Agostino, ANCR WG Chair
- 14 • Sharon Polski
- 15 • Paul Knowles

16 Reviewers:

- 17 • Gigi Agassini, ANCR WG Secretary

ANCR: Digital Transparency Performance Scheme

32	Conformity & Compliance Assessment v0.9.9.....	1
33	NOTICE.....	3
34	Conditions for use.....	3
35	Dear reader,.....	5
36	Abstract.....	6
37	Scheme Applicability.....	6
38	1 Terms & Definitions.....	8
39	Normative to Council of Europe, Convention 108+,.....	8
40	Introduction.....	9
41	Why was this specification written?.....	10
42	Why Transparency Performance Indicators?.....	11
43	About the Scheme.....	11
44	The TPIs here are used to assess session-based data capture and self-asserted information	
45	by organizations to specify a Public level of Trust Assurance that is provided in an online	
46	context.....	12
47	TPI 1 - Measuring the Timing of PII Controller Identity Notification:.....	13
48	TPI 2 - Measures Required Data Elements.....	13
49	TPI 3 - Measure of Transparency Accessibility.....	14
50	TPI 4: A Measures security information integrity.....	15
51	TPI Metrics.....	16
52	Table 1: Transparency Performance Rating.....	16
53	Table 2: Transparency Performance Indicator Record Rating Example.....	18
54	Summary.....	19
55	Appendix A: TPI Compliance Assessment Scheme Part 2.....	20
56	A.1 Operational Transparency Assessment.....	20
57	Appendix B: TPI Assessment Guidance.....	21
58	B.1 TPIs are captured in sequence.....	21
59	B.2 TPI – Scheme 1, Part 1(S1-P1) metric logic.....	22
60	B.3 1.2. Table 2 : ANCR Record Schema Example.....	23
61	Appendix C: Digital Transparency Code of Conduct.....	24
62	Endnotes.....	24
63		
64		

ANCR: Digital Transparency Performance Scheme

65

66 **IPR Option:**

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

71 Any derivative use of this specification must be in conformance with the associated
72 transparency Code of Conduct¹, be open and free and not create any dependency that
73 limits or restricts the use, accessibility, and availability of digital transparency or the
74 ability for the PII Principal to provide and manage their own consent.

75 **Suggested Citation: (upon WG approval)**

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

77 NOTICE

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

82

83 **Conditions for use**

84 License Condition: This specification is solely used for assessing conformance to the
85 Transparency Code of Conduct (Appendix C), for implementing the Council of Europe
86 108+ Chapter III, Rights of the Data Subject, Section 1 Transparency, and modalities,
87 Article 14, 1 – 8. This Transparency Code of Conduct is internationally representative of
88 notice and consent legal and social requirements. It can be represented today in the
89 form of privacy policy links, physical signage, digital cookies and security or privacy
90 notices. These are found when accessing public and digital service spaces, in all
91 domains and jurisdictions, and are to be referenced as practices, which MUST
92 implement, or support the implementation of this Transparency Code of Conduct for
93 transparency modalities.

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

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

ANCR: Digital Transparency Performance Scheme

94

95 This document has been prepared by participants of Kantara Initiative Inc ANCR-WG.
96 Permission is hereby granted to use the document solely for the purpose of
97 implementing the Specification for public benefit. No rights are granted to prepare
98 derivative works of this Specification. Entities seeking permission to reproduce this
99 document, in whole or in part, for other uses must contact the Kantara Initiative to
100 determine whether an appropriate license for such use is available.

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

112

ANCR: Digital Transparency Performance Scheme

113 Dear reader,

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

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

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

128

129 Copyright: The content of this document is copyright of Kantara Initiative, Inc.
130 © 2023 Kantara Initiative, Inc.

131

132

133

134

135

136

137

138

139

140

141

142

143

ANCR: Digital Transparency Performance Scheme

144 Abstract

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

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

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

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

169 Scheme Applicability

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

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

ANCR: Digital Transparency Performance Scheme

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

ANCR: Digital Transparency Performance Scheme

194 1 TERMS & DEFINITIONS

195

196 Normative to Council of Europe, Convention 108+,

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

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

203

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

206

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

210

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

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

212

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

215

216

ANCR: Digital Transparency Performance Scheme

217 Introduction

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

222

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

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

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

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

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

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

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

252

253 Why was this specification written?

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

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

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

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

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

277

ANCR: Digital Transparency Performance Scheme

278 Why Transparency Performance Indicators?

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

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

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

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

298

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

302 About the Scheme

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

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

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

ANCR: Digital Transparency Performance Scheme

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

317

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

321

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

325

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

331

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

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

341

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

ANCR: Digital Transparency Performance Scheme

342 TPI 1 - Measuring the Timing of PII Controller Identity

343 Notification:

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

- 347 i) Before,
- 348 ii) At the time of,
- 349 iii) During, or
- 350 iv) After

351 Personally identifiable information is captured.³

352

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

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

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

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

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

364 TPI 2 - Measures Required Data Elements

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

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

Commented [SD1]: Reference to be inserted

ANCR: Digital Transparency Performance Scheme

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

374 The following Digital Privacy transparency elements are the minimum required to
375 operationalize transparency and accountability.

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

390 TPI 3 - Measure of Transparency Accessibility

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

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

402

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

ANCB: Digital Transparency Performance Scheme

403 TPI 4: A Measures security information integrity

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

411

ANCR: Digital Transparency Performance Scheme

412 TPI Metrics

413 Transparency Performance Rating

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

419

420 For TPI 1:

- 421 • +1 refers to the existence of a technical framework and PII Controller
422 transparency **prior** to the initiation of a session. This provides security-based
423 trust assurances for the data subject.
- 424 • 0 refers providing dynamic transparency in context **at the start** (which is at the
425 time of collection), including purpose and other required disclosures,
- 426 • -1 refers to where the legally required information is presented at some point in
427 the session.
- 428 • -2 refers to the provision of low quality legally required information.
- 429 • -3 refers to the provision of non-operable, non-compliant, unusable
430 transparency and digital privacy related information.

431 For TPI 2

- 432 • +1 is given for each of the Controller information of the elements
- 433 • -3 if the information is missing.

434 For TPI 3

- 435 • +1 for meeting legal requirements for responsiveness for each of the required
436 PII Controller information categories.
- 437 • -2 for response but not within legal requirements
- 438 • -3 if information unavailable

439 For TPI 4

- 440 • +1 for the contextual integrity of each the security features
- 441 • 0 if information available but not immediately or easily accessible
- 442 • -3 for each integrity mismatch

443

444

ANCP: Digital Transparency Performance Scheme

445 Table 1: Transparency Performance Indicator Record Ratings

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

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

ANCR: Digital Transparency Performance Scheme

447 Table 2: Transparency Performance Indicator Record Rating
448 Example

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

449

450

451

ANCR: Digital Transparency Performance Scheme

452 Summary

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

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

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

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

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

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

474

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

ANCR: Digital Transparency Performance Scheme

APPENDIX A: TPI COMPLIANCE ASSESSMENT SCHEME PART 2

A.1 Operational Transparency Assessment

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

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

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

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

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

ANCR: Digital Transparency Performance Scheme

504 APPENDIX B: TPI ASSESSMENT GUIDANCE

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

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

514

515 B.1 TPIs are captured in sequence

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

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

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

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

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

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

ANCR: Digital Transparency Performance Scheme

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

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

ANCR: Digital Transparency Performance Scheme

532

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

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

536

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

ANCR: Digital Transparency Performance Scheme

537 APPENDIX C: DIGITAL TRANSPARENCY CODE OF 538 CONDUCT

539 These digital transparency code of conduct rules coincide with the TPIs presented and
540 reference the international adequacy requirements for transparency required for digital
541 identifier management. In [Report on the Adequacy of Digital Identity Governance](#) for cross
542 border transparency and consent:

543

544 PII Controller must:

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

552 Endnotes

553

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

556

557