Transparency Performance Scheme and Indicators (TPIs)

Enhancing Digital Trust by Publishing TPIs, and Developing a Consensus Protocol to Promote Conformance and Compliance to International Law, Standards and Best Practice

Develop the Basis for a Conformance and Compliance Program

- Existing assurance programs are focused on data protection and are not human centric and as a result are not well suited to address transparency, notice, and consent requirements from an international business, operational, legal, technical or social perspective.

- The Transparency Performance Scheme and Indicators are specification and conformance program based on legal requirements that exist across regimes and specifically referenced in CoE 108+

Promote the Work and Roadmap

- Share Scheme, TPIs, and Controller Credential Conformance/Compliance framework internally with Kantara LC and WGs.

- Coordinate with WGs in NIST presentation/outreach as input to:
  - SP 800-63-4 (Transparency?)
  - Identity Roadmap
  - Cybersecurity and Privacy Frameworks

- [22 September event](#) in coordination with new Quebec Privacy laws

- Coordinate with ISO WG on 2756x related efforts.

TPIs

1. Timing of PII Controller Identity Notification
   - Before
   - At time of
   - During
   - After
2. Required Data Elements - Content of Notice
   - Is the legally contextual required information present?
   - Organization(s), PII Controller(s), DPO PoC, Purpose, Justification

TPIs

3. Transparency Accessibility - Access to Rights and Information
   - Immediate, Link, Request and Time to Respond, At the end of a long trail

4. Security Information Integrity
   - How are things secured?
     - PKCS
     - JWT
     - …
   - Does it align with notice and risk?
     - Subject, Location, Policy, Privacy and Security Controls

Scheme Applicability

1. All processing must be transparent.
2. This is true for all stakeholders and delegates.
3. All processing requires a record of privacy notice and policy, a record of consent
4. Records and receipts act as a record of processing activity (ROPA), CoE108+, Article 31.
5. A notice receipt can be created by any stakeholder.
6. Anchored Notice and Consent Receipt can be used to access data subject right and as co-regulation tool.