Notice Record & Receipt Information Structure

This is a wiki page for discussion. (not official group specification) Please join the call and request access for the latest draft

Status of this document

- Outlined Draft v0.4

This international and internet scalable information structure references and contributes to multiple work efforts, the record fields are from ISO/IEC 29100 Privacy and Security Techniques, which is a free ISO/IEC standard.

This framework references multiple on-going efforts. Governance driven -Business, Legal Technical interoperability for people with what is broadly describe as legally defined consent.

1. ANCR Record (Consent Receipt Pre-fix)
    a. Concludes
2. ISO/IEC 27560 WD3 - (Consent Receipt v1.1)
3. W3C Data Privacy Vocabulary Controls CG v0.5 (legal to machine readable)
4. 0PN-AuthC: Protocol
5. Code of Conduct & Practice
    a. for example a transparency code of conduct, for notice, notification and disclosure defaults

Related efforts

1. DIACC special interest group, and records and receipt profile for the PCTF.

Specification Overview

The scope and focus of this work group is to work on part 1 of the Notice Record, Notice Receipt and Consent Notice Receipt information structures and contribute this towards the international record and receipt specification.

The full record and receipt information structure specification is framed with 5 sections which are being worked on by different community groups and efforts also introduced in this overview.

Sections are as follows

1. Anchored Notice Record
2. Purpose Specification
3. Data Control, Protection and Treatment
4. Code of Conduct & Practice
5. Advanced Notice and Consent Receipt Record
    a. Consent Receipt Prefix. is being specified with inputs from Verified Credential community of work via ToiP

Specification Roadmap

Section 2, 3, & 4 - are being specified by a combination of other efforts including ISO 27560 which are all happening in 2021-23 time frame,.

Section 5 - Is the specification of field for the record and receipt specification, which we aim to contribute towards a global privacy rights access standard in the future.

Section Summaries

Section 1: Anchored Notice Record

A key element missing in online only interactions is proof of informed or knowledgeable consent and the risks associated with this notice. The objective is to work through the fields in sections and to specify a way to generate consent receipts by both PII Principal and PII Controller.

By working through the first ANCR Record section we aim to complete the first deliverable, in which a report will be made and the next section can be reviewed. The ANCR record starts at the beginning of the information structure to create an open record.

Section 1: topics under review

1. Dynamic Data Controls
2. Dynamic Fields:
    a. default consent types for the ANCR Record
3. Generating a Receipt for another legal justification
4. generating a receipt under the authority of a) PII Principal, b) PII Controller, c) Both

5. Privacy Rights Agreement - Specifying the legal privacy rules according to the jurisdiction
6. Jurisdiction of PII principal for determining rights access. (right to complain and be heard)
7. Adding a notice payload to a consent receipt
8. Rendering a receipt to display the proof of notice
9. Rendering the receipt to display notification
10. Rending a receipt for privacy rights access information.
    a. Default notice rendering
    b. Verifying rights access and performance
    c. PII Principle is a verified claim when provided by the individual.
    d. How can this claim be verified

Section 2: Purpose Specification

In the Consent Receipt v1.2.2 section focus and discussion on the consent record information structure, utilizing the GDPR an Internationally adopted (ISO 29184) legal processing justification categories

1. purpose specification fields (are for the most part the same as v1.1)
2. purpose context - legal justification of processing - instance(s) of processing, purpose categories,
3. purpose specification for 6 legal justifications
4. specifying rights requests and data processing controls
5. The rights are then listed with the legal justification in the next sections of the receipt.

The GDPR rights specification are used here for example, as a privacy agreement enforced in many countries it provides the current International standard for privacy rights.

Note: A consent receipt can be specified for only one legal justification and one purpose (or purpose bundle).

Section 3: Data Control, Protection & Treatment

This section is an expansion of the receipt fields to further specify the scope of the legal processing of personal information for a specified purpose. Assuring a purpose limitation principle.

of Provides the fields for the technical capture of personal data processing, separating storage, access and privacy rights that apply for the specified legal justification and context.

This section focus discussion on.

- additional fields for specifying privacy rights that are available and the scope of permission that are accessible to the PII Principle.
- Consent Grant Conditions
- Withdraw Permission for a Consent Grant
- Privacy Rights Applicable for this processing context
- Notice of Risk and Liabilities Required in place (or in addition) to contract terms or license agreements
- Notifications : the required notice, notifications, and disclosures for valid processing. This is a new section, which is in early review and development.
- Privacy/ Security - Change & Notification Log, required for records of processing, for open, operational and responsive Online privacy notification.

Section 4: Code of Conduct & Practice (Optional)

Extending the Privacy Agreement (or legislation) with a technical code of conduct or practice, which can be notified with a badge and icon, provide transparency over additional safeguards and measures (aka privacy preserving technology) that provide additional privacy assurances, in addition to a more streamlined privacy service user experience.

Discussion includes:

1. A code of conduct, which extends privacy legislation and is approved by a privacy regulator.
2. a code of practice, which extends a specified purpose with additional codified practices which are either specified by the Notice Controller, or with a certified and audited/auditable practice.

These additional options can be used to bundle like purposes together, specify each purpose for a consistent and standard processing, streamline experiential use by presenting enhanced practices with a valid/authorised badge, icon, or micro-credential. .

Section 5: Field Input Data Field Sources (UNCL)

The specification of the field data for each section will be collated and combined, including the data sources and specified and referenced according to the OECD Guidelines, Standards, regulatory guidance and legislation.

The long term aim of this section is to **U**nify the **N**otice **C**ontrol   **L**anguage (**UNCL**) iterating towards a notice centric Ontology. Mapping privacy agreement vocabularies with the ISO 29100 terms and definitions and W3C Data Privacy Vocabulary, for machine readable semantics.

Unified fields data - for purpose specification which harmonizes context - for decentralized governance referring to a consent by default status.

		Section 5: Consent Receipt Field Inputs v0.1 record spec - with specified field data - which then harmonizes what is specified as a consent for a purpose - ./		
Field Label	Reference	**Field Input: Source, and list**	Example	Required
Accountable Person Role		Defined according to privacy agreement GDPR: Data Protection Officer, Data Protection Representative, and translated to ISO. As role – Chief Privacy Officer, with comparable responsibilities		
Consent Type		There are a number of legal consent types which are required for active state consent transparency and compliance 1. implied consent - e.g. going to a website 2. implicit consent - e.g. through actions that are implicit and indicative of consent expectations 3. explicit consent - e.g. providing personal information for a legal specified purpose and privacy rights notice (assumes meaningful and informed digital consent) 4. expressed (or directed) consent - e.g. an explicit consent that is specified by the PII Principal 5. altruistic consent - e.g. a consent specified with a code of practice rather that to a specific legal entity (name of controller not necessarily provided)		
Sensitive (or Special) PII Category		Sensitive Personal Data Categories • personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; • trade-union membership; • genetic data, biometric data processed solely to identify a human being; • health-related data; • data concerning a person’s sex life or sexual orientation. **References** • Article 4(13), (14) and (15) and Article 9 and Recitals (51) to (56) of the GDPR		
Personal Data Categories		Personal Data Categories - these have been contributed to the W3C Data Privacy Vocabulary Controls where they are synced and maintained		
		Note: add delegated authority types • Note - add notification types • Note - list of things that go into privacy log - to maintain a valid state of processing / consent • Note- Add what collections methods are usable for receipt		

JSON-LD Example (TBD)

In Progress

Generating a Consent Receipt

1. Generate a Notice Record,
   a. this is created from the assessing the notice information, presentation, layered information and policy
2. Generate a Notice Reciept
   a. once the record is generated assess the record with a conformance profile specified from ISO 29184, or from regulation or international practice
   b. generate receipt, which is a digital twin of the notice record, and include the results from this assessment aimed to providing rights information and access
3. Generate a Consent Notice Receipt.
   a. Utilizing the Notice Receipt, specify which rights, and generate a consent notice receipt for the PII Controller,
4. Receiving a Consent Notice Reciept
   a. There are multiple ways to source, validate and verify the valid state of privacy signalled with the record and receipt
   b. All of the technical information and records of processing are linked to the receipt and is usable to automate the response.

ANCR Record & Blinding Identity Taxonomy for Consent Receipt Identifier Management

Their are 2 identifiers used in the receipts

1. is the ANCR Record iD which is anchored to the PII Controller Notice and the PII Principal's capture of the notice (or equivalent)

2. The Consent receipt iD that is generated when a PII Principle interacts with the notice, context of a sign or notification

Acronyms

BT = Blinding Taxonomy is a field that is encrypted, and blinded, so as not be available at rest without a key, in this specification, these fields are blinded by the PII Principal's User Agent. (BUAT) If these fields are generated by a 3rd party or controller, then this data is not 'required' in this is specification.

Glossary (WiP)

To View Glossary and Terms - request access for the WG Leadership.

Evidence of Consent

Privacy Agreement

Proof of Notice

Consent Grant for a Purpose

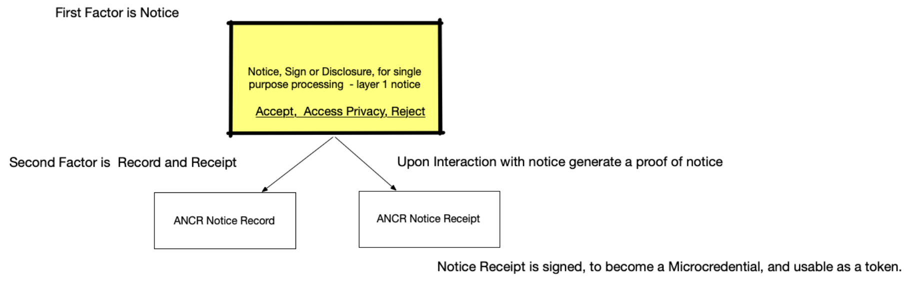
Purpose Limitation (and Scope)

Permissions for a Purpose

Purpose (or Permission) Management - Not Consent Management Platforms - (there is no such thing as consent management platform - this is permission management at best)

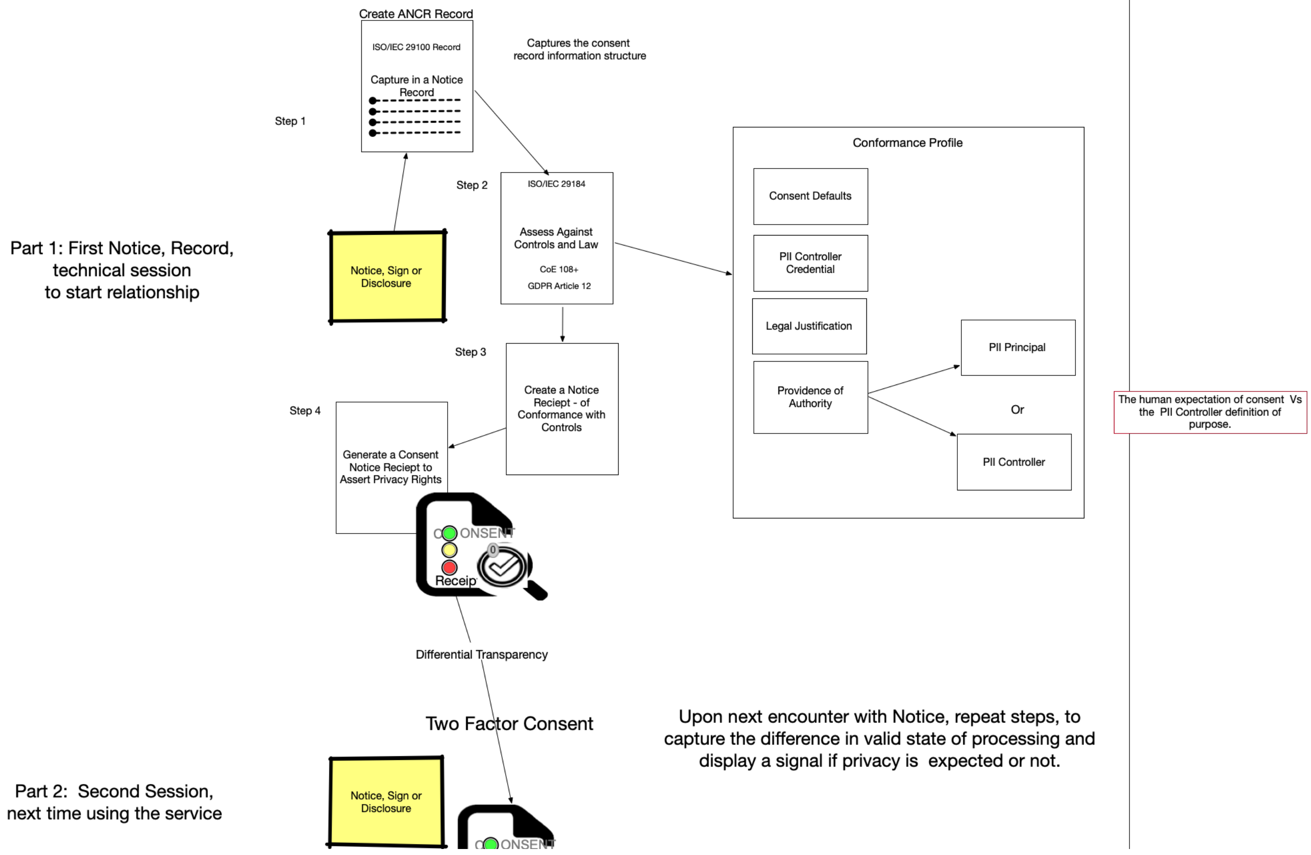
Generate - or collect a Notice upon arrival at a website
- create a notice record
- generate a consent receipt token
- replace cookies with tokens
- use differential transparency as notice context for shared understanding
- browser/plugin/wallet - can produce notice automatically using International ISO/IEC 29100 Records and Receipts

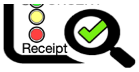
Two Factor Notice (2fN)


First Factor is Notice
Notice, Sign or Disclosure, for single purpose processing - layer 1 notice
Accept, Access Privacy, Reject
Second Factor is Record and Receipt
Upon Interaction with notice generate a proof of notice
ANCR Notice Record
ANCR Notice Receipt
Notice Receipt is signed, to become a Microcredential, and usable as a token.

Differential Transparency

Independent privacy signal generated for any context for privacy as expected is a human consent gateway


Create ANCR Record
ISO/IEC 29100 Record
Capture in a Notice Record
Captures the consent record information structure
Step 1
Step 2
ISO/IEC 29184
Assess Against Controls and Law
CoE 108+
GDPR Article 12
Conformance Profile
Consent Defaults
PII Controller Credential
Legal Justification
Providence of Authority
PII Principal
Or
PII Controller
The human expectation of consent Vs the PII Controller definition of purpose.
Part 1: First Notice, Record, technical session to start relationship
Notice, Sign or Disclosure
Step 3
Create a Notice Reciept - of Conformance with Controls
Step 4
Generate a Consent Notice Reciept to Assert Privacy Rights
CONSENT
0
Receip
Differential Transparency
Two Factor Consent
Upon next encounter with Notice, repeat steps, to capture the difference in valid state of processing and display a signal if privacy is expected or not.
Part 2: Second Session, next time using the service
Notice, Sign or Disclosure
CONSENT



Part 3: Differential Transparency

When receipts are compared a notice is generated on
when there is a change in the valid state of consent