Consent Receipt v1.2 Framework Roadmap

This is a wiki page for discussion. (not official group specification)

Status of this document

- Outline Draft

Summary Overview

V1.2 - updates towards dynamic data control record and receipt information structure.

We are now working on and discussing ANCR v1.2.1 - ANCR record Specification

Section Summary

Background

The Consent Receipt v1.2 is specified for devoting scalable and dynamic data processing controls and authorizations with privacy rights. It is based on the OECD Guidelines on the Protection of Privacy and the Transborder Flows of Personal Data and is apart of a body of work for privacy standards and assurance developed over the 20 + years. and guided the harmonization of privacy law in the EU and internationally. The OECD Guidelines is closely tied with the Council of Europe's CoE 108+ (an international privacy agreement), and importantly ISO/IEC 29100, which is interpreted as a security framework extension to encompass the scope of privacy in information technology.

The OECD guidelines are formalized with the ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework, for common terms and definitions, further made accessible as it is released as A Public ISO Document. Providing a mature and common semantic framework to refer to the privacy stakeholder relationships in notice and consent records.

The Consent Receipt v1.2 is the culmination of work over the last 5 years updating the v1.1. The V1.2 is better described here as a record of a Privacy Notice and is specified using the OECD Guidelines through the use of ISO/IEC 29100.

The receipt is generated upon interacting with a Privacy Notice so that a person can capture evidence of reading a notice, and be used to assess conformance to privacy law, or with ISO/IEC 29184:2020 Online Privacy Notice and Consent standard, which has published the Consent Notice Receipt v1.1 in Appendix B.

Consent by Default (for Dynamic Data Control)

The ANCR record re-works the flow so as to start with a valid state of Consent, which is then consumed by identity management technologies. Changing the flow of surveillance and enabling people to human-trust the use of surveillance and enable a flow of consensual data processing to dramatically decrease and minimize the requirements for privacy notice and notifications.

The user experience and Receipt v1.2 is referred to as a Consent by Default because the initial relationship state for any interaction is provided by default in relation to what is reasonably expected by the purpose and context of use by the individual as specified in law.

From this starting point, and legitimate legal justification can then be used to dynamically assert a control over the data that is controlled by the individual. For example the consent default which intiaites the data flow may be implied consent, and an Contract, or the Vital Interests of the data subject might be used, with a verified PII Controller, or Privacy Controller Credential, (see ToiP - Privacy Controller Credential Specification)_ to dynamically access the personal data. ANCR Notice record can be generated for proof of notice. Consent Receipt can be generated for evidence of legitimate processing for another legal justification.

Consent Types

The ANCR record provides the PII Controller and PII Principle digital identifiers and context along with a consent type, which provides a default scope of permissions in a consent grant to a system.

The consent types here aim to express the full range of consent defaults expected and will evolve.

Consent Type	Description	Defaults to Apply	Permission Scope for digital Identity system
Explicit Consent			
Implied Consent			
Expressed Consent			
Directed Consent			

Altruistic Consent			

Specifying Notice Record and Receipts for Additional Legal Justifications

Any additional legal justification can be Notified from this default context and instance to generate and link a consent receipt. An Anchor Record is generated from the PII Controllers credentials as displayed.

Producing a proof of notice for any additional legal justification can be used to update the default for that context to a new legal justification produced with a notice, notification or disclosure. The Consent Receipt is used as a digital twin of the consent notice in which the legal justification (if not consent) is signalled to be presented to the PII Principle to inform of the data processing.

Note: The consent receipt is used to capture the use of the legal justification for a specified and specific purpose. One legal justification and one purpose (or purpose bundle) per Consent Receipt.

Specification Draft

Appendix A: Full Specification Overview

The scope and focus of this workgroup is to work on 1 part of the consent record information structure, and contribute this towards a developing global record and receipt specification.

The full record and receipt specification is framed with 5 sections which are being worked on by different groups and efforts and is the Appendix (below).

The focus of this workgroup on the first section is aimed at creating a Proof of Human Notice for digital Evidence of processing for dynamic data controls for digital identifiers.

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 aim 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 section and complete the first deliverable a report will be made and the next section can be reviewed.

In this section we aim to review these topics.

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 & Surveillance 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 experiencial 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 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. A receipt is generated from the information on the ANCR Record, which is also the pre-fix of the consent receipt
    a. There are multiple ways to source and verify the information is valid and active in an ANCR record, before it is used to generate a consent receipt
2. The default state of a notice record is consent, it is further specified with additional legal justifications, which are overlaid upon the default state, or specified as an explicit consent to a specified purpose, which is captured by the notification provided by the PII Controller

Note: For PasE protocol - all Stakeholders generate a consent receipt for each processing activity

1. in the processing a Consent Receipt is created for each PII Processing activity for a PII Controller by each Process and Sub-Processor using a 2 Factor Notice protocol in which a notice is generated first time a purpose or processing is authorized, approved by the accountable person, to generate a derogated consent receipt for that specific stakeholder, retrievable by a PII Principle with the consent receipt id, (only when) the ANCR id is generated from a consent receipt id provided by the PII Controller

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

Definition of terms and their references from ISO, W3C etc

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)