Privacy Controller Credential & UNCL (Unified Notice Control Language)

Notice & Consent for people relies on clear communication. Decentralized identity relies on legal semantics to express technical semantics that are mirrored to provide data governance that people expect. Data governance referring explicitly to the transborder use of personal information and personal identifiers. As there are no standardized legal semantics for Digital identity and personal Transborder data management presents a challenge. This work aims to develop a Unified Notice Control Language, that utilizes the OCA and the W3C Data Control Vocabulary (mapped legal ontology) to harmonize decentralized legal semantics, utilizing the International Kantara Notice & Consent Receipt specifications (now in WD2 ISO 27560) and ISO 27984. Online Privacy Notice and Consent standard.	**Notice & Consent Task Force** **Project owner:** Mark Lizar Salvatore D'Agostino **Team members:** **Ken Adler**	**Status** ACTIVE

Overview

Decentralized Data Governance for Data subject's (data) rights

1. A key challenge, which is addressed with an International standards, is the lack of semantic harmonization for personal data control which provides security for the portability and control of private information and is a required for people to be able to independently consent and control personal information. This challenge, which was originally championed by the Open Notice Initiative's Presentation and Paper @ the W3C DoNotTrack Conference in Berkeley California. 'Opening Up the Online Infrastructure' called for collaboration on the semantic standards to be developed. Ultimately realizing that intention data governance standards were needed, and international data governance policy was required to govern between jurisdictions, technical domains, and identity management systems. It was also abundantly clear, the only legal, and human centric framework for this Internationally, is Notice & Consent. Notice and Consent, after an exhaustive research campaign, Notice, and semantics are the only consistent legal, technical and socially required component, for all contexts dealing with personal information.
2. This turned into a Kantara Specification effort in 2014 and now, last year, ISO voted to fast track this to a standard 27560, to be used with ISO 29184 to address what was know by the phrased of the Biggest Lie on the Internet, was a focus of a movie Terms and Condition's May Apply. With an international governance rule set, people can use independently of Terms and Conditions.
3. With the success of this work as an international standard this Task Force aims to collaborate to support an International data governance authority framework as an open resource for master data control transparency over personal information (with standardized notice).

Specification Outline

1. Overview of (OPN) Data Governance Authority Architecture:
    a. Intro
        i. This data governance authority architecture provides the international legal roles for
    b. Identity & Data Governance Legally Specified Actors /Stakeholders
        i. Policy Controller, Privacy (Data) Controller, Registration Operator Governance Authority, DGA - Registrar
    c. Privacy Risk Assurance Levels 1-4
        i. Policy Controller, Privacy Controller, Data/Identity Governance Authority Operator (DGAO)
            1. Controller: Tier 0 Risk Assurance - Not Registered
            2. Policy Controller (or just Controller) - Tier 1 Assurance - Self Asserted Binding -No Privacy Risk Assurance - Discoverable
            3. Privacy Controller (or Data Controller) - Tier 2 Assurance - Signed Binding for Legal Compliance - Mitigated Risk Assurance
            4. Data Governance Authority Operator - Tier 3 - Assurance - High Risk Assurance
            5. Registrar - Tier 4 - Registrar Infrastructure -
                a. Low Risk Personal Data Processing -
                    i. only personal information of Controller, and Company Operators
2. Privacy Controller Credential Specification
    a. Overview: a Privacy Controller Credential is comprised of a bound relationship identifiers for accountability and transparency: This enables data supply chain transparency
        i. Accountable Person + Legal Entity Identifier
            1. Legal Status of Accountable person and Legal Entity
            2. Wether the Accountable person is employed by Legal Entity, or 3rd Party
                a. if 3rd Party - Privacy Controller Credential of 3rd party is required
        ii. Conditions of access and use:

1. the accountable person info should be masked unless required (not published as is required in some jurisdictions)

3. Use Case(s)
    a. Digital Immunisation Passport
    b. Legal Justifications for processing
        i. Surveillance of identifiers
        ii. Holder, Verifier & Issuer

Unified Notice Control Language for Semantic Harmonization

UNCL:

Uses the definitions and terms specified in the ISO 29100 framework, Consent Receipt v1.2, for specifying key roles for data control, transparency and accountability. This international framework is the basis for extending semantic data governance to decentralized data economy. In this economy, the Privacy Controller Credential extended the Privacy Controller Public Profile for verified claims, decentralized identifiers, and Self Soverign applications. For this purpose, this specification is used to provide the best practices for the data controller to generate a verifiable credential, the considerations in using this as a legal credential for standardized data processing.

The Privacy Controller, the accountable, authorizing stakeholder for data processing is the key audience for this specification and language.

Key Problem>

At this time, a high risk, high sensitivity data processing activity, has the responsibility to be transparent over the legal entities responsible for processing personal data, the beneficiaries of the data processing activity, in addition to any othe processors. This includes partners and data processing service providers, like Google or identity management service provider.

This privacy controller profile, printed out in long form would have multiple legal entities and Privacy Controller Credentials required, this would include all of their mailing addresses (by law) and , public contact point/addresses, and the details of any jurisdictional representative for privacy and data protection.

This specification, aims to tease out the language used for specifying these elements, which are legally required to be Public so that they can be represented with a single distributed identifier to simplify each DDE interaction.

Privacy Risk Assurance ;

- refers to trustworthy transparency
    - e.g does this organization use of standardized legal semantics for notice and consent to ease understanding

Requirements Privacy Controller Credential Specification (in Open Consent Groups' OPN Architecture)

Providence chain starts with the person who is accountable bound to a legal entity.

Legal Entity Accountability Levels according to Tiers of Privacy Risk

Tier 0 - No-Risk Indicated : Self Asserted Binding with a privacy policy - providing minimum Privacy Risk Assurance (trustworthy Transparency)

- A non registered Broadcast listing

Tier 1 - Policy Controller - Low Risk - doesn't process personal data electronically, does not collect or process personal information, and for any personal identifier, this is minimized and secure, has internal security for data of employee's

Tier 2 - Privacy (data) Controller - Does process personal data for commercial benefit and use

Tier 3 - Very High Risk - invisible public surveillance, surveillance of children /vulnerable people etc Beneficial owners (required)

Tier 4 - Controller Operator - Provides Registration services for Privacy Controller Credentials, Mitigates Privacy Risk with codes of conduct and certifications that accredit codes of practice. Controller can then register to these codes of conduct and practice

Use's of The PCC Credential - a single identifier for a Privacy Controller, which links to all LEI's for beneficial ownership.

- Simplify Transparency
- Improve performance
- Sign Receipts to create tokens
- Provides
    - Privacy - Transparency over legal entities, accountable people and beneficial -
    - Legal Entity Identifier Purpose and Sources
        - to identify the legal entity of the privacy controller
        - beneficial owner of the legal entity

- Accountable Person Role
    - to identify the accountable person / role that is bound to the legal entity identifier (aka) organization.
        - could be an employee
        - owner / director / officer
        - data proaction officer
        - 3rd. Party Company Representative
            - accountable role - (for another 3rd Party) acting representative

- Privacy Controller
    - under what authority
    - under what legal justification

ISO 29100 Privacy Stakeholders

Privacy Stakeholders	ISO Definition	
Regulator /		
PII Principal		
PII Controller		
PII Processor		
3rd Party		

Privacy Controller Credential Roles			
Data Governance Authority Operator Role	Certification Providers on Regulator Approved Codes of Conduct - very limited PII - data controller personal information and a linked reference to a data subjects identifier -		
Data Governance Registrar	`		

Stakeholder	Privacy Controller Credential : Creating Credentials for a use Case	Description	
	Issuer		
	Holder		
	Verifier		

Gov ToiP Role	UseCase Example	Roles	Actors Privacy Stakeholders ▪ controller, processor, subject, 3rd Parties	
	Provides the schema - hospital	issuer	Privacy Controller	
	Person - Requesting Information from - patient/traveller	holder	Data Subject	
	3rd Party - border control	Verifier	Data Processor / 3rd Party	

- looking to make a process for what Legal Privacy Stakeholder has the Credential Role
    - Steps to assign Stakeholder Roles
        - Test for checking if its a processors or a 3rd party?

Legal Semantic Element	semantic description	functional usage	fields Required	
controller				
controller_identity				

controller address registered				
controller address (mailing)				
controller contact	extend consent termination for a control point			

Delegated Role :

			Delegated
Regulator			Ombudsman
PII Principal			Guardian
PII Controller			Joint-Controller
PII Processor			Sub-Processor
3rd Party			turtles

References for use for creating a Unified (generic) Data Control Vocabulary for OCA

Standard /Specifications	Title	Description	Resource Status
ISO 29100	Information technology — Security techniques — Privacy framework	ISO/IEC 29100:2011 provides a privacy framework which • specifies a common privacy terminology; • defines the actors and their roles in processing personally identifiable information (PII); • describes privacy safeguarding considerations; and • provides references to known privacy principles for information technology.	Status - Is publicly available - https://www.freestandardsdownload.com/iso-iec-29100-2011.html
ISO/IEC 29184: 2020	Online privacy notice and consent		(just published - not available to public - we are working on publishing a report /appendix for use with this group)

W3C DPV 0.01	Data Privacy Vocabulary	• legal ontology for technically breaking down and mapping legal ontology to a data legal ontology -
		• the Notice + CR V1.2 and W3C DPV, also use a common set of purpose categories. and the Kantara CR v1.1 for purpose specification
		• (note shared by initial FIHR approach - now much more evolved)
			• active -
			• additional information
			  • Background: EU Funded Project Special
			  • Creating a Vocabulary

Topic List

Topic Title		
Risks		
Mapping Governance	Matching with ToiP Governance	

References

Topic	Link	

Risks	Identity and Verifiable Credential Risks	

Reference Implementations

Implementer			
Human Colossus			
OpenConsent			
I_Grant			

OPN: Open Notice (+ Consent) Receipt Schema: Starters Guide to Unified Data Control Schema

Lizar, M. & Pandit, H.J., OPN: Open Notice Receipt Schema, 14th International Conference on Semantic Systems (SEMANTiCS 2019), Karlsruhe, Germany, 2019 [Published http://www.tara.tcd.ie/handle/2262/91576 [accessed July 1, 2020]

Field Name	Field Label	Format	Description	Required /Optional
Schema Version	version	string	The version of specification used to which the receipt conforms. To refer to this version of the specification, the string "v1" or the IRI "https://w3id.org/OPN/v1" should be used.	Required
OPN Privacy Profile URI	profile	string	Link to the controller's profile in the OPN registry.	Required
Type of Notice Receipt	Notice Receipt	string	Label Notice Receipt	Required
Receipt ID	id	string	A unique number for each Notice Receipt. SHOULD use UUID-4 [RFC 4122].	Required
Timestamp	timestamp	integer	Date and time of when the notice was generated and provided. The JSON value MUST be expressed as the number of seconds since 1970-01-01 00:00:00 GMT (Unix epoch).	Required
Signing Key	key	string	The Controller's profile public key. Used to sign notice icons, receipts and policies for higher assurance.	Optional
Language	language	string	Language in which the consent was obtained. MUST use ISO 639-1:2002 [ISO 639] if this field is used. Default is 'EN'.	Optional
Controller Identity	controllerID	string	The identity (legal name) of the controller.	Required
Legal Jurisdiction	jurisdiction	string	The jurisdiction(s) applicable to this notice	Required
Controller Contact	controllerContact	string	Contact name of the Controller. Contact could be a telephone number or an email address or a twitter handle.	Required
Link to Notice	notice	string	Link to the notice the receipt is for	Optional
Link to Policy	policy	string	Link to the policies relevant to this notice e.g. privacy policy active at the time notice was provided	Required
Context	context	string	Method of notice presentation, sign, website pop-up etc	Optional
Receipt Type			The human understandable label for a record or receipt for data processing. This is used to extend the schema with profile for the type of legal processing - and is Used to identify data privacy rights and controls	

OCA schema specification: *https://docs.google.com/spreadsheets/d/1KOdq8Yy3OXmuELyh7tpHMlhyMZPSZ3Ib/edit#gid=68769926*