GDPR: Explicit Consent Record & Receipt Extension for [Kantara CISWG: Consent Receipt](https://kantarainitiative.org/confluence/download/attachments/76447870/Consent%20Receipt%20Specification%201_1_0%20DRAFT%208%20-%20clean.docx?version=1&modificationDate=1519153788000&api=v2)  v1.1

**Ext. Title**: GDPR Explicit Consent Record & Receipt Extension for [Kantara CISWG: Consent Receipt](https://kantarainitiative.org/confluence/download/attachments/76447870/Consent%20Receipt%20Specification%201_1_0%20DRAFT%208%20-%20clean.docx?version=1&modificationDate=1519153788000&api=v2)
**Status:** (in draft: for a Kantara proposal for certification and conformance program)

Methodology (Project Kit) for creating this consent receipt extension can be found[**here**](https://kantarainitiative.org/confluence/pages/viewpage.action?pageId=104600510)**.**

# **Objective of this CR Extension**

The Consent Record & Receipt, GDPR Extension for extending the [Kantara CISWG:(MVCR) Consent Receipt v1.1](https://kantarainitiative.org/confluence/download/attachments/76447870/Consent%20Receipt%20Specification%201_1_0%20DRAFT%208%20-%20clean.docx?version=1&modificationDate=1519153788000&api=v2) is to map the GDPR lexicon to the international ISO 29100 lexicon.

Intended use:  Used as a core format for an authoritative record and receipt format that contains all the consent elements in the GDPR for the most explicit consent for special categories of data, including children’s (and vulnerable peoples) data as required in the GDPR.

This Extension is used to map the European General Data Protection Regulation terms and explicit consent compliance requirements to the Kantara Initiative Consent Receipt (CR) v1.1. Mapping to a common record and receipt output so as to harmonise privacy, compliance and evidence requirements necessary to create authoritative privacy records.

In this extension document, only those elements that have been mapped or added to the Consent Receipt Specification, are specified in this extension document.

This document defines the field mappings to replace terms and glossary items in the CR v1.1. specification, this specification also adds additional fields and terms, that are required by the GDPR as an extension to the CR v1.1,

# **Extension Scope**

This extension to the Kantara CR V1.1 map's the EU GDPR lexicon to the international ISO lexicon for explicit consent, while also adding extension fields to meet GDPR requirements.

This extension provides an example of how to generate an extension for the Kantara (Minimum Viable Consent Receipt Specification) Consent Receipt v1.1 that maps a national legislation to an international open standard, to enable interoperability in use of explicit consent records internationally.

This extension interprets the Kantara Consent Receipt v1.1 specification as an explicit consent record and receipt specification that is used by the Identity Management industry to specify a high assurance explicit consent token.

This extension interprets the GDPR ‘justification for consent’ as 'explicit' for specified 'special categories' of personal data, including the recoding of delegated explicit parental consent for the processing of children's data, services which process special categories of personal data, employ automatic identification, decision making and profiling.

For fields for an explicit consent receipt the 'Equivalent' GDPR field name replaces the MVCR field name and is used to replace the terms and fields in the CR.

Scope Limitation: The notice and policies required for this explicit consent and their conformance should be linked via the required Data Controller URL and are not in scope of this extension.

## ****An Explicit Consent Record for Producing a Receipt****

This specification extension acknowledges that an explicit consent receipt is made with a subset of fields in a consent record. This extension provides some guidance for keeping records of processing by defining the fields and format for creating a consent record that demonstrates compliance with GDPR records of processing and proof of notice requirements for an explicit consent receipt, and in so doing, meet the requirements as set out in Article 12 and 30 of the Regulation.

Creating a record of consent for an explicit consent receipt. The explicit consent record should include, the processors, sub-processors, delegated consenting parties contact name and address, and fields with the required linked contracts, model clauses and agreements, linked to the record of consent, which are not represented in the receipt fields provided to the Data Subject. In addition, onward transfers, in a record of consent that produces a receipt, the onward transfer should include the country being transferred to, list type of safeguard, and provide a link to a url with a description of the transfer.

Records are required for explicit consent on behalf of the processor, this will be required if the Controller is audited, or if the controller is seeking accreditation for high assurance explicit consent to mitigate high privacy risk. In such context, these records should include the categories of recipients the nature and purpose of the processing, the type of personal data and categories of data subjects, and the duration of storage, which is required to be present in the processor record for consent as defined in Article 28 (3).

For regulator and bodies providing codes of practices or accreditation, an explicit consent record requires Art 30 1(d) the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations; Including, the category of data subjects – is required in a consent record along with the data category, as required in records of processing Article 30 1(c)

## Section 1: New and replacement terms in the extension

|  |  |  |  |
| --- | --- | --- | --- |
| GDPR Term | GDPR Definition | CR v1.1 Term | CR v1.1 Definition |
| Consent | ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; (A4-11) | Consent | A Personally identifiable information (PII) Principal’s freely given, specific and informed agreement to the processing of their PII (ISO 29100) |
| Data Subject | Identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. (A2-a) | PII Principal | The natural person to whom the personally identifiable information (PII) relates. NOTE: Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym “data subject” can also be used instead of the term “PII principal.” (ISO 29100 - PII Principal) |
| Data Controller | ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; (A4-7) | PII Controller | A privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes. NOTE: A PII controller sometimes instructs others (e.g., PII processors) to process PII on its behalf while the responsibility for the processing remains with the PII controller. (ISO 29100) Note: may also be called data controller. |
| Data Processor | ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; (A4-8) | PII Processor | A privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller. (ISO 29100) |
| Personal Data | ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (A4-1) | Personally Identifiable Information (PII) |  |
| Right to Withdraw Consent | The data subject shall have the right to withdraw his or her consent at any time. (A7-3) | Termination | --- |

### Categories of controller

#### GDPR Definition:

the categories of processing carried out on behalf of each controller; Article 30 (2b)

The reason the Data Controller is collecting the Personal Data.
Associations and other bodies representing *categories of controllers* may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, Art 40.2

#### CR V1.1 Term Replaced:

Purpose Categories

The reason the PII Controller is collecting the PII. Example Purpose Categories currently in use are available on the Kantara Consent & Information

Categories of Processing

#### GDPR Definition:

* + - the categories of processing carried out on behalf of each controller; Article 30(2b)
		- the purpose of processing or the categories of processing Art 23 2 (a)

#### CR V1.1 Term Replaced:

* + - purpose categories in

Categories of data subjects

#### GDPR Definition:

* + **Art.301(c) a description of the categories of data subjects and of the categories of personal data; 1(d)the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;**

#### CR V1.1 Term Replaced:

Categories of recipients

#### GDPR Definition:

* + record Art 30 1(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
	+ Receipt
		- the recipients or categories of recipients of the personal data, if any;

#### CR V1.1 Term Replaced:

* + CR – 3rd party disclosure are required in Article 13 1 (e) “This is required via the recipients or categories of recipients of the personal data, if any;

### Consent Type: Explicit Consent Only

#### GDPR Definition:

This extension is for the Explicit consent type only and is defined in Article 6.1(a) as a justification for the processing of personal data. In which, the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

#### CR V1.1 Term Replaced:

### The type of the consent used by the PII Controller as their authority to collect, use or disclose PII. The field MUST contain a non-empty string and the default value is “EXPLICIT”. But can also include, implied,

### Controller

#### GDPR Definition:

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

*Source: GDPR Art 4(7)*

#### CR V1.1 Term Replaced:

##### PII Controller:

A privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes.

*Source: ISO 29100*

#### Noticed Difference:

TBD.

### Data Subject

#### GDPR Definition:

An identified or identifiable natural person.  An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

*Source: GDPR Art 4(1)*

#### CR V1.1 Term Replaced:

##### PII Principal:

The natural person to whom the personally identifiable information (PII) relates.

*Source: ISO 29100*

#### Noticed Difference:

Difference is that it is not only identified, but expands scope to identifiable. Referring to any data that can be personal (not just identified personal data)

### Erasure (Harsh)

#### GDPR Definition:

#### Article 4 (2)

#### CR V1.1 Term Replaced:

### International transfer

#### GDPR Definition:

* + **(Art 45) Art 46**
	+ **Us transference internationally (6) (25) (101) (110 -BCR) Art 3(3) Note: International transfer: exemption Not applicable for orgs with 250 or less staff. Unless specific context (Privacy Risk) is warranted**

#### CR V1.1 Term Replaced:

### International Transfer Safeguards

#### GDPR Definition:

* + - Safeguards need to fall into one of the following categories, Guidance Art 46.2
		- (a) a legally binding and enforceable instrument between public authorities or bodies;
		- (b) binding corporate rules in accordance with Article 47;
		- (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
		- (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
		- (e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
		- (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

#### CR V1.1 Term Replaced:

### Onward transfer

* + **is there an onward international transfer of personal data? (Art 44)**
	+ **the documentation of suitable safeguards; Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.**

### On-Behalf

#### GDPR Definition:

* + on-behalf or delegation to a representative
		- is referred to in GDOR for the data Controller, Processor, Data Subject and Regulator
		- Recital 74,79, 80

#### CR V1.1 Term Updated (not Replaced)

####  On Behalf extends the CR specification terminology with

### Processor

#### GDPR Definition:

A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

*Source: GDPR Art 4(8)*

#### CR V1.1 Term Replaced:

##### PII Processor:

A privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller.

*Source: ISO 29100*

#### Noticed Difference:

these are equivalent

### Personal Data

#### GDPR Definition:

Any information relating to an identified or identifiable natural person ('data subject')

*Source:  GDPR:Art 4(1)*

#### CR V1.1 Term Replaced:

##### Personally Identifiable Information (PII):

Any information that (a) can be used to identify the PII Principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII Principal

*Source: ISO 29100*

#### Noticed Difference

these are equivalent

### Profiling

#### GDPR Definition:

* + **60) Art 4,(4)**

CR V1.1 Term Replaced:

### Processing

#### GDPR Definition:

any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

*Source:  GDPR:Art 4(2)*

#### CR V1.1 Term(s) Replaced:

##### Processing of PII

An operation or set of operations performed upon personally identifiable information (PII).

*Source: ISO 29100*

* + USE
		- Any processing of personal data done by a Personal Data Controller or by a PII processor on behalf of a PII Controller. Processing In the GDPR the term Processing maps to the term USE. Note: to CR Editor processing on behalf of processor is termed sub-processing and should be amended in the CR v1.1 spec, Optional, String

#### Noticed Difference

these are equivalent

### Special Categories of Data

#### GDPR Definition:

*Source GDPR Art 9*

Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation

#### CR V1.1 Term Replaced:

##### Sensitive PII:

Sensitive Categories of personal information as defined in regulation (or potentially by the PII Principal), either whose nature is sensitive, such as those that relate to the PII principal's most intimate sphere, or that might have a significant impact on the PII principal. These categories are specified as sensitive in FIP's based legislation and refer specifically to racial origin, political opinions or religious or other beliefs, personal data on health, sex life or criminal convictions and require opt-in informed consent.

*Source: ISO 29100*

#### Noted Difference

these are equivalent

### Security

* + **\*1.'Take into account the state of the art for security, the costs of implementation and key considerations. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:' a.Does the systems use pseudonymisation and encrypt personal data? b.Does the system have the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services? c.Is there the ability to restore the availability and access to personal data in a timely manner in the event of physical or technical incident? d.Is there a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing? e.Does the system adhere to an approved code of conduct or certification mechanism to which security compliance can be audited?**

### Sub-processor

####  GDPR Reference

#### GDPR References sub-processors in this way, but lacks operational clarity which is why the new term is introduced.

Article 28.3(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
Art28.4"
"Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations."

clarity is required so that liability can be crystal clear between processor and sub-processor as the Processor is 100% liable for the sub-processor " Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations."Art28.4" in the GDPR. Which requires a contract which provides the same rights as the GDPR, or similar framework

#### Referred to in the GPDR is "another Processor" (recital 109) or "other than Initial Processor" Art 28.4

####  CR v1.1 Reference

#### Referenced in CR at

### Withdraw Consent & Erasure

### GDPR Reference

### Recital 39 In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure

### CR v1.1 Term Replaced

* Termination:

## Section 2: Table 1 fields mapped to the CR v1.1

### Section 2.1 Fields about Consent Receipt

#### Section 2.1.1 Changed/Existing Fields from CR v1.1

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CR v1.1 Field Name** | **Equivalent GDPR Term** | **GDPR CR Field Name** | **GDPR Field Description (Put in examples)­­­** | **JSON** | **Required / Optional** | **Data Type** |
| Version | N/A | Version | The version of the specification to which a receipt conforms.  The value MUST be "xxxxxx" for this version of the specification. | version | Required | String |
| Jurisdiction | N/A | Jurisdictions | Jurisdiction(s) applicable to this transaction. This field MUST contain a non-empty list of strings describing the jurisdiction(s). Each string in the list MUST describe a country (using ISO 3166) or a legislative region (such as EU). | jurisdictions | Required | Array |
| Consent Receipt ID | N/A | Receipt ID | A unique number for each Consent Receipt. SHOULD use UUID-4 [RFC 4122]. This field MUST contain a non-empty string. | receiptID | Required | String |

#### Section 2.1.2 Added Fields

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Field Name** | **Guidance** | **Description** | **Data Types (define field format)** | **JSON** | **Required / Optional** |
| Receipt Timestamp | This field specifies the timestamp at which the receipt was generated/provided to the data subject. This timestamp can be separate from the timestamp of the given consent. | Date and time of the receipt. The JSON value MUST be expressed as the number of seconds since 1970-01-01 00:00:00 GMT. ISO 8601 Date and Time Format [ISO 8601] MUST be used for formatting. | receiptTimestamp | Optional | Number |

### Section 2.2 Fields about Consent

#### Section 2.2.1 Changed/Existing Fields from Cr v1.1

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CR v1.1 Field Name** | **Equivalent GDPR Term** | **GDPR CR Field Name** | **GDPR Field Description (Put in examples)­­­** | **JSON** | **Required / Optional** | **Data Type** |
| Consent Timestamp | N/A | Consent Timestamp | Date and time of when consent was given by the data subject. The JSON value MUST be expressed as the number of seconds since 1970-01-01 00:00:00 GMT. ISO 8601 Date and Time Format [ISO 8601] MUST be used for formatting. | consentTimestamp | Required | Number |
| Collection Method | N/A | Collection Method | A description of the method by which consent was obtained. | collectionMethod | Required | String |
| Language | N/A | Language | Language used to obtain consent. MUST use ISO 639-1:2002 [ISO 639] if this field is used. | language | Optional | String |
| PII Principal ID | Data Subject | Data Subject ID | Identifier used to denote the Data Subject’s identity for consent e.g. email address, phone number.  | dataSubjectID | Required | String |
| Consent Type |  | Consent Type | Type denotes nature of given consent in its relation to the data subject. In this extension the default value is "EXPLICIT” | consentType | Required | String |
| Termination | Right to Withdraw Consent | Withdraw Consent | Information about withdrawing consent according to rights provided by the GDPR. | withdrawConsent | Required | String |

#### Section 2.2.2 Added Fields

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Field Name | Guidance | Description | Data Types (define field format) | **JSON** | **Required / Optional** |
| Data Subject is Child | This field is used to specify if the data subject is a child | The age for a child differs by jurisdiction. | Boolean | **isChild** | **Required** |
| Given By Delegation | This field is used to specify if the consent was given by delegation | If data subject is a child, their consent may required to be given by their parent or guardian in certain cases | Boolean | **delegation** | **Optional** |
| **Delegate Identity** | This field denotes the identity of the delegate in the delegation. | This is the identity (such as name, email) of delegate that provides consent on behalf of the data subject in the delegation. Required if consent given by delegation. | String | **delegate** | **Optional** |
| **Delegate Role**  | This field is used to specify the authority used to represent the party in the consent transaction  | Role played by the delegate in the delegation. E.g. “parent of child”. Required if consent is given by delegation. | String | **delegateRole** | **Optional** |
| **Consent ID** | This field is used to specify the internal consent ID used by the Controller to refer to consent | Controllers may wish to provide this for convenience in their communication with the data subject for referring to this specific consent. | String | **consentID** | **Optional** |
| **Validity** | This field is used to specify the validity or duration of consent after which the consent can no longer be used as a legal basis. | The validity can be a specific date-time, or a duration (e.g. 6 months), or based on an event or condition (as long as account is valid) | String | **validity** | **Required** |
| **Rights** | This field is used to specify how the data subject can exercise their rights under the GDPR | Rights include Right to Rectify, Right to Data Portability. The Right to Withdraw is specified in the “withdrawConsent” field. | Array | **rights** | **Required** |

### Section 2.3 Fields about Data Controller

#### Section 2.3.1 Changed/Existing Fields from Cr v1.1

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CR v1.1 Field Name** | **Equivalent GDPR Term** | **GDPR CR Field Name** | **GDPR Field Description (Put in examples)­­­** | **JSON** | **Required / Optional** | **Data Type** |
| Public Key | N/A | Verification Key | Cryptographic key used to verify the receipt’s integrity. Can be Controller’s Public Key in the context of encrypted information. | verificationKey | Optional | String |
| PII Controller |  | Collected By | Consent can be collected by another entity on behalf of the Controller, which can be specified by this field. The field is optional, and its absence indicates the consent was collected by the same Controller as defined in the receipt.  | collectedBy | Optional | String |
| PII Controllers | Data Controller Article 4 (7) | Controllers | Identities of the Controllers to whom the consent is applicable. Each item in the list of Controllers must specify the identity, website, contact, DPO, and policies for that Controller. | Controllers | Required | Array |
| PII Controller URL |  | Controller Website | The website of the Controller. | controllerWebsite | Optional | String |
| PII Controller Contact | see Data Controller | Controller Contact | Contact details of the Controller. There can be multiple contacts such as phone number, email, twitter handle. Each contact must be accompanied with a description of its type e.g. @acmeinc (twitter) | controllerContact | Required | Array |
| Privacy Policy |  | Policies | Links to the Data Controller's policies such as privacy statement/policy and applicable terms of use in effect when the consent was obtained, and the receipt was issued. If a policy changes, the link SHOULD continue to point to the old policy until there is evidence of an updated consent from the Data Subject.   | privacyPolicy | Required | Array |

#### Section 2.3.2 Added Fields

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Field Name | Guidance | Description | Data Types (define field format) | **JSON** | **Required / Optional** |
| Controller | This field is used to specify the identity of the Controller | An identity is the legal name of the organisation.  | String | **controller** | **Required** |
| Controller DPO Contact | This field is used to specify the contact details of the Controller’s DPO | There can be multiple contacts such as phone number, email, twitter handle. Each contact must be accompanied with a description of its type e.g. @acmeinc (twitter) | Array | **controllerDPO** | **Required** |

### Section 2.4 Fields about Purposes, Processing, and Personal Data

#### Section 2.4.1 Changed/Existing Fields from Cr v1.1

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CR v1.1 Field Name** | **Equivalent GDPR Term** | **GDPR CR Field Name** | **GDPR Field Description (Put in examples) ­­­** | **JSON** | **Required / Optional** | **Data Type** |
| Purposes |  | Purposes | The receipt can contain one or more purposes that provide explanation for the processing of personal data.  | purposes | Required | Array |
| Purpose |  | Purpose | A short, clear explanation of why the personal data is required to be processed. Each purpose should specify the personal data, sensitive personal data, processing categories, data storage, involved third parties, international transfers, profiling, and automated decision making. | purpose | Required | String |
| PII Categories | Personal Data (PD) Category | Personal Data | A list of Personal Data Categories required for use in the specified Purpose. Each category should be well defined and published - such as in code of practice. Each Purpose can have one or more categories of personal data associated with it. Categories that are sensitive should be listed in the Sensitive Personal Data field. | personalData | Required | Array |
| Sensitive PII | special categories of personal data  | Sensitive Personal Data | A list of Sensitive Personal Data Categories required for use in the specified Purpose. Each category should be well defined and published - such as in code of practice. Categories that are not sensitive should be listed in the Personal Data field. | sensitivePersonalData | Optional | Array |
| Third Party Disclosure | Processor, Third Party | Third Parties | Indicates if the Data Controller is disclosing Personal Data to a third party for the specified purpose. Each listed third party or third-party category in the list must have a role associated with it e.g. Processor, Law Agency. | thirdParties | Required | Array |
| Third Party Name | Processor, Third Party | Third Party | The name the Third Party the Controller will disclose the Personal Data to. Must be accompanied by the role e.g. Processor. | thirdParty | Required | String |

#### Section 2.4.2 Added Fields

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Field Name | Guidance | Description | Data Types (define field format) | **JSON** | **Required / Optional** |
| Third Party Role |  | Describes the role of the third party to whom data is disclosed for the specified purpose e.g. Processor or Partner | String | **thirdPartyRole** | **Required** |
| International transfer  | This field is used to indicate if personal data is transferred outside GDPR-applicable jurisdictions | The field indicates that the specific purpose involves transfer to a jurisdiction not under GDPR | Boolean  | **internationalTransfer** | **Required**  |
| International transfer locations | This field is used to indicate the locations the personal data will be transferred to that are not under the jurisdiction of the GDPR | Must use a normative form for the location such as ISO country codes or taxonomies for unions and region abbreviations (e.g. EU, EEA). Required if international transfer field is true. | Array | **internationalTransferLocations** | **Optional** |
| International transfer safeguards  | If international transfer is yes – list in the array which safeguards are used.  | Required if international transfer field is true. | Array | **internationalTransferSafeguards** | **Optional**  |
| Profiling | This field is used to indicate if the specified purpose involves profiling | In GDPR, ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements; | Boolean | **profiling** | **Required** |
| Automated decision making | This field is used to indicate if the specified purpose is solely based on automated measures that produce legal effects for the data subject | This is mentioned in GDPR as decision based solely on automated processing, including profiling, which produces legal effects for the data subjects or similarly significantly affects him or her. | Boolean | **automatedDecisionMaking** | **Required** |
| Processing Categories | This field is used to list the processing categories associated with a purpose. | Describes the data processing actions/activities carried out over personal data for the specified purpose. E.g. collect, use, store, share. | Array | **processing** | **Required** |
| Data Storage | This field is used to specify the data storage duration or conditions associated with the purpose. | The data storage field can specify the date/time or duration, or a condition or event (e.g. as long as account is active) after which the data will be erased and will no longer be used for the specified purpose | String | **dataStorage** | **Required** |

#### Section 2.5 Removed Fields

|  |  |
| --- | --- |
| **CR v1.1 Field Name** | **Reason for removal** |
| On Behalf | Information represented using Delegation and Collected-by fields.  |
| Primary Purpose | Primary Purpose would be covered by Legitimate Interest as the legal basis |
| Purpose Category | Categories of purposes are not required, is covered by Purpose |
| PII Controller Address | Is covered by Controller Contact |
| PII Controller Email | Is covered by Controller Contact |
| PII Controller Phone | Is covered by Controller Contact |
| Services | Service is covered by Purpose |
| Service | Service is covered by Purpose |

##

# ****Section 4: Schema****

{

 "$schema": "http://json-schema.org/draft-07/schema#",

 "type": "object",

 "required": [

 "version",

 "jurisdictions",

 "receiptID",

 "consentTimestamp",

 "collectionMethod",

 "dataSubjectID",

 "consentType",

 "withdrawConsent",

 "isChild",

 "validity",

 "rights",

 "controllers",

 "purposes"

 ],

 "properties": {

 "version": {

 "type": "string"

 },

 "jurisdictions": {

 "type": "array",

 "items": {

 "type": "string"

 }

 },

 "receiptID": {

 "type": "string"

 },

 "receiptTimestamp": {

 "type": "string"

 },

 "consentTimestamp": {

 "type": "string"

 },

 "collectionMethod": {

 "type": "string"

 },

 "language": {

 "type": "string"

 },

 "dataSubjectID": {

 "type": "string"

 },

 "consentType": {

 "type": "string"

 },

 "withdrawConsent": {

 "type": "string"

 },

 "isChild": {

 "type": "boolean"

 },

 "delegation": {

 "type": "boolean"

 },

 "delegate": {

 "type": "string"

 },

 "delegateRole": {

 "type": "string"

 },

 "consentID": {

 "type": "string"

 },

 "validity": {

 "type": "string"

 },

 "rights": {

 "type": "array",

 "items": {

 "type": "string"

 }

 },

 "verificationKey": {

 "type": "string"

 },

 "collectedBy": {

 "type": "string"

 },

 "controllers": {

 "type": "array",

 "items": {

 "type": "object",

 "required": [

 "controller",

 "controllerWebsite",

 "controllerContact",

 "controllerDPO",

 "policies"

 ],

 "properties": {

 "controller": {

 "type": "string"

 },

 "controllerWebsite": {

 "type": "string"

 },

 "controllerContact": {

 "type": "array",

 "items": {

 "type": "string"

 }

 },

 "controllerDPO": {

 "type": "array",

 "items": {

 "type": "string"

 }

 },

 "policies": {

 "type": "array",

 "items": {

 "type": "string"

 }

 }

 }

 }

 },

 "purposes": {

 "type": "array",

 "items": {

 "type": "object",

 "required": [

 "purpose",

 "personalData",

 "sensitivePersonalData",

 "processing",

 "dataStorage",

 "thirdParties",

 "internationalTransfer",

 "profiling",

 "automatedDecisionMaking"

 ],

 "properties": {

 "purpose": {

 "type": "string"

 },

 "personalData": {

 "type": "array",

 "items": {

 "type": "string"

 }

 },

 "sensitivePersonalData": {

 "type": "array",

 "items": {

 "type": "string"

 }

 },

 "processing": {

 "type": "array",

 "items": {

 "type": "string"

 }

 },

 "dataStorage": {

 "type": "string"

 },

 "thirdParties": {

 "type": "array",

 "items": {

 "type": "object",

 "required": [

 "thirdParty",

 "thirdPartyRole"

 ],

 "properties": {

 "thirdParty": {

 "type": "string"

 },

 "thirdPartyRole": {

 "type": "string"

 }

 }

 }

 },

 "internationalTransfer": {

 "type": "boolean"

 },

 "profiling": {

 "type": "boolean"

 },

 "automatedDecisionMaking": {

 "type": "boolean"

 }

 }

 }

 }

 }

}

**Example Document**

**{**

 **"version": "2.0",**

 **"jurisdictions": [**

 **"EEA"**

 **],**

 **"receiptID": "c0fbfbd3-f380-4cb4-a4f9-328621c3824d",**

 **"receiptTimestamp": "1551959162",**

 **"consentTimestamp": "1551959162",**

 **"collectionMethod": "website",**

 **"language": "en",**

 **"dataSubjectID": "john.doe@example.com",**

 **"consentType": "EXPLICIT",**

 **"withdrawConsent": "https://example.com/",**

 **"rights": [**

 **"https://example.com/"**

 **],**

 **"isChild": false,**

 **"validity": "90 days",**

 **"delegation": true,**

 **"delegate": "jane.doe@example.com",**

 **"delegateRole": "Spouse",**

 **"consentID": "9adf514a-3a77-415c-86a0-569c075ee547",**

 **"verificationKey": "66D6EBEEF47B5D6D421417874BDC9A5F9A8FD2D1C881FAAB7EF21EC02FB40D67",**

 **"collectedBy": "Acme-B Inc.",**

 **"controllers": [**

 **{**

 **"controller": "Acme Inc.",**

 **"controllerWebsite": "https://example.com/",**

 **"controllerContact": [**

 **"acme@example.com (email)",**

 **"+0-000-0000 (phone)",**

 **"@acme (twitter)"**

 **],**

 **"controllerDPO": [**

 **"acme-DPO@example.com (email)",**

 **"+0-000-0001 (phone)",**

 **"@acmedpo (twitter)"**

 **],**

 **"policies": [**

 **"https://example.com/privacy-policy",**

 **"https://example.com/t&C"**

 **]**

 **}**

 **],**

 **"purposes": [**

 **{**

 **"purpose": "Show Personalised Ads",**

 **"personalData": [**

 **"name",**

 **"location"**

 **],**

 **"sensitivePersonalData": [**

 **"health-data"**

 **],**

 **"processing": [**

 **"observe",**

 **"record",**

 **"analyse"**

 **],**

 **"dataStorage": "6 months",**

 **"thirdParties": [**

 **{**

 **"thirdParty": "Ad Generator",**

 **"thirdPartyRole": "Processor"**

 **}**

 **],**

 **"internationalTransfer": false,**

 **"profiling": true,**

 **"automatedDecisionMaking": false**

 **},**

 **{**

 **"purpose": "Manage Delivery of Goods",**

 **"personalData": [**

 **"name",**

 **"address",**

 **"phone-number"**

 **],**

 **"sensitivePersonalData": [],**

 **"processing": [**

 **"collect",**

 **"use"**

 **],**

 **"dataStorage": "2 months after delivery is completed",**

 **"thirdParties": [**

 **{**

 **"thirdParty": "Delivery",**

 **"thirdPartyRole": "Partner"**

 **}**

 **],**

 **"internationalTransfer": true,**

 **"internationalTransferLocations": [**

 **"USA"**

 **],**

 **"internationalTransferSafeguards": [**

 **"encryption"**

 **],**

 **"profiling": false,**

 **"automatedDecisionMaking": false**

 **}**

 **]**

**}**

# ****Summary****

* This specification specifies the required fields for a consent receipt to demonstrate compliance with a code of conduct
* Specifies receipt that enables withdrawal of consent as easlily as provided with a notice of time to erasure of data
* Specifies receipt enables the assertions of required security
* Specifies receipt enables explicitly high assurance transfer of liability and specifies delegated parties
* Specifies receipt once conformance demonstrates companies with notice and record compliance in Article 12 and 30
	+ **Compliance Statement: Record of Processing**
	+ **This receipt demonstrates compliance with Article 12, notice and Article 30 records of processing in the GDPR**
	+ **The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.(art 30 -3)**
* Specifies receipt

# ****Appendix****

Appendix

Input into Kantara CISWG

Questions

* Action to WG to update the json field names to a more neutral set, that are more widely understood.  I.e. from pii\_controller to controller
* Can the WG - Clarify PII Controller URL - as company website URL - not the privacy policy URL - required to verify controller against policy

Field Analysis

**On-Behalf Field :**

The On Behalf field was first written in as Consent on behalf of the PII Principle, which covered explicit consent by a parent or guardian for children, but how to do this was unclear at the time - so we decided to wait until an explicit example could be made for completing the specification of the on behalf field.   (Note to Harsh; On-Behalf can be replaced with a term like – delegated party or agent)

* The on-behalf field has been one of a handful of long standing action items

Now it is currently in the spec as an optional field for acting on behalf of-  but, in the spec earlier it refers to - acting on behalf of the data controller as a  data representative, with 3 contravening references.

1. On-Behalf field in the CR v1.1 shows an example that defines a sub-rpocess and processor – which is already defined as a 3rd party in the spec – which meand this field is redundant in the CRv1.1 – once a sub-processor field is defined.
2. The aforementioned - consent on behalf of PII Principle
3. Line 212 - in the spec referring to  PII Controller having someone (or a 3rd party org) act on their behalf as a data representative -  which arguably could also be required of a Data Processor
4. Then as a delegated processor -
	1. Line 264 — Use - includes  in its description to processing on behalf of a processor  on be-half of a
	2. Line 331 - OPTIONAL: A PII Processor acting on behalf of a PII Controller or PII Processor. For example, a third-party analytics service would be a PII Processor on behalf of the PII Controller, or a site operator acting on behalf of the PII Controller.

The way it is currently referred to in Line264 and 331 I would assert is no longer correct since the GDPR as what was termed   ‘on behalf’ in the UK Privacy Act, now is directly referred to as a Processor. The term processor now encompasses that personal data is being processed on behalf of a controller.   should not refer to processing - which, in the CR v1.1 spec is also defined as USE (line 263) and should correctly be termed in the context of delegated consent role - i.e. acting or consenting  on behalf of - for the explicit purpose of administering or the processing of an explicit consent.

This reviewed definition still leaves outstanding the example that is now defined in the current spec in Line 331 - as outlined by the use case of a ‘third-party analytics service’  which is a different but closely related field issue and reveals the gap in the CR v1.1 specification, where there is a missing term - ’sub-processor’,

Note: this can be even more  confusing as marketing industry  is making the case for their sub-processing to be understood as a  joint controller instead. - making the requirement to add sub-processing explicitly even more clear at this time

Solution:

To further specify the above on-behalf field in the GDPR Extension, as well as to specify explicitly the processing of children data as a new field defined in the GDPR Extension,

Specifying

1. a term that maps ‘on behalf’ to Sub-Processor for use in the GDPR
2. Adding the Term On-Behalf as a new term in GDPR term Section
	1. As ‘a party acting on, or consenting on the behalf of; a PII Principle, controller, processor or regulator.  And should be used as such.
3. Adding fields for specifying who the -on-behalf- party is-
	1. name, address, contact, role and authority

On-Behalf - CRv1.1 : GDPR extension, spec

* Map on-behalf from CR v1.1 to GDRP extension as sup
	+ The on-behalf field in the CR is mapped to Sub-Processor in the Extension
* And in the GDPR Fields section
* The On-Behalf Field
	+ is further defined in this extension to represent
		- Consent or Acting On-behalf of  the PII Subject, controller, processor or Regulator
	+ The representing party
		- Name, address, contact,
		- role, For
			* PII Subject
				+ A Parent, Guardian, Advocate or Agent
			* Controller
				+ Data Protection Officer, Data Controller Representative
			* Regulator
				+ Approved Auditing and Certification frameworks
		- Authority
			* A URL link (or inclusion of) a certificate of authority or approved verification

Applied to the GDPR Extension

(A GDPR field is added in the GDPR Extension section: )

* If Children’s Data is being processed = Yes
	+ Consent On Behalf, field is used
		- Consent on behalf
			* With the selected role of parent or guardian
* If a 3rd party representative is provisioning or administering explicit consent on behalf of  controller, processor, then
	+ Acting on behalf, to process consent with the role of
		- Data Protection Officer, Data Protection Representative
* if Regulator
	+ Acting on behalf, is with the role of
		- Approved Trusted 3rd party that is accredited by the regulator

# Sub-Processor

# Sub-processing and compliance for international data transfers, the identity of sub-processor if PII is transferred internationally, may be required in circumstances of explicit consent for special categories of data and delegation of consent for children consent depending on the personal data and processing context and if there is any harm to the PII Principle the liability of sub-processing is lightly touched upon in that Marketing Enterprise i.e calling 3rd Party Analytics a service being run as a Joint Data Controller - instead of a sub-processor - clarity is required so that liability can be crystal clear between processor and sub-processor as the Processor is 100% liable for the sub-processor " Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations."Art28.4" in the GDPR. Which requires a contract which provides the same rights as the GDPR, or similar framework