Consent Receipt Specification

Version: 1.1.0

Document Date: 2018-02-20

Editors: Mark Lizar, David Turner

Contributors: Richard Beaumont, Chris Cooper, Sal D'Agostino, Rupert Graves, Iain Henderson, Mary Hodder, Harri Honko, Andrew Hughes, Tom Jones, Robert Lapes, Oliver Maerz, Eve Maler, Jim Pasquale, Samuli Tuoriniemi, John Wunderlich

Produced by: Consent & Information Sharing Work Group

Status:

This document is a Kantara Initiative Technical Specification Recommendation produced by the Consent & Information Sharing Work Group, and has been approved by the Group. The Public Comment and Intellectual Property Rights Review has been completed. It has been approved by the Membership of the Kantara Initiative. See the Kantara Initiative Operating Procedures for more information.

Abstract:

A Consent Receipt is record of authority granted by a Personally Identifiable Information (PII) Principal to a PII Controller for processing of the Principal's PII. The record of consent is human-readable and can be represented as standard JSON. This specification defines the requirements for the creation of a consent record and the provision of a human-readable receipt. The standard includes requirements for links to existing privacy notices & policies as well as a description of what information has been or will be collected, the purposes for that collection as well as relevant information about how that information will be used or disclosed. This specification is based on current privacy and data protection principles as set out in various data protection laws, regulations and international standards.

IPR Option:

Patent & Copyright: Reciprocal Royalty Free with Opt-Out to Reasonable And Non-discriminatory (RAND)

Suggested Citation:

Consent Receipt Specification 1.1.0. Kantara Initiative Consent & Information Sharing Work Group. 2018-02-20. Kantara Initiative Technical Specification Recommendation. https://kantarainitiative.org/file-downloads/consent-receipt-specification-v1-1-0/

NOTICE

55 **Contents**

76

1 INTRODUCTION

Current regulations and best practices for privacy protection include requirements for notice and consent. There is no standard or specification for an interoperable consent record. As a result, neither individuals nor organizations can easily track their consents or know who to hold accountable in the event of a violation of their consent.

Individuals are regularly asked for consent by organizations who want to collect information about them, usually in conjunction with the use of a service or application. Consent is provided by an individual when they agree to allow an organization to collect, use, or disclose their data, and data about them, according to a set of terms and conditions defined by the collecting organization.

A record of a consent enhances the ability to maintain and manage permissions for personal data by both the individual and the organization. Much like a retailer giving a customer a cash register receipt as a record of a purchase transaction, an organization should similarly create a record of a consent interaction and give it to the individual, defined here as a Consent Receipt (CR), to memorialize this interaction in a way that is useful to people. The creation and implementation of this standardized format will promote consistent consent practices, support consent management interoperability between systems, and enable proof of consent.

The CR elements described in this specification represent privacy-related requirements common to many jurisdictions. A JavaScript Object Notation (JSON) schema for a CR is included to enable interoperable data exchange and processing. The specification includes extension points so that implementors can incorporate information required for their particular regulatory and policy requirements.

The OECD Guidelines [OECD], Council of Europe Convention, and European Union Data Protection Directive [EU-DATA] relied on Fair Information Practices (FIP) as core principles. Due to the international and cross-domain use of a Consent Receipt, this document refers to the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [OECD] focusing on consent using the ISO 29100 [ISO 29100:2011] lexicon.

2 NOTATIONS AND ABBREVIATIONS

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", “NOT RECOMMENDED”, "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119].

All JSON [RFC 7159] properties and values are case sensitive. JSON data structures defined by this specification MAY contain extension properties that are not defined in this specification. Any entity receiving or retrieving a JSON data structure SHOULD ignore extension properties it is unable to understand. Extension names that are unprotected from collisions are outside the scope of this specification.

The following abbreviations are used:

CR	Consent Receipt
FIP	Fair Information Practices
GDPR	General Data Protection Regulation
JSON	JavaScript Object Notation
JWT	JSON Web Token
PI	Personal Information
PII	Personally Identifiable Information

3 TERMS AND DEFINITIONS

This specification uses terminology and definitions from *ISO/IEC 29100:2011 "Information Technology -- Security techniques -- Privacy Framework"* [ISO 29100:2011] and other published, FIP-based best practices, to maintain consistency with the terms commonly used in regulations. If a jurisdiction's terms are not compatible with this specification, these internationally-defined terms can be mapped to localized terms. For example, PII Principal in this document maps to the term Data Subject in European legislation. For ease of mapping and use, this document will define those terms for clarity and specificity for this specification.

Although this specification uses the ISO 29100 lexicon, its use of this language is not normative, and the terms should be replaced according to the jurisdiction that regulates its provision. The JSON field names are normative. The specification is based on privacy and data protection principles as set out in various data protection laws, regulations and international standards.

Collection

Receiving, creating, or obtaining data from or about a PII Principal.

Disclosure

The transfer, copy, or communication, by a PII Controller or a PII Processor acting on behalf of the PII Controller, of PII and accountability for that PII when transferred to another entity, which will become the PII Controller of that PII.

NOTE: When a PII Controller transfers or copies information to another entity it retains accountability for that PII. An example would be an entity using a cloud storage service for backups. We note this here because, for a PII Principal, both this 'use' and actual 'disclosure' may be termed 'sharing' information. However, there are significant differences from a transparency and regulatory point of view.

Consent

A Personally identifiable information (PII) Principal's freely given, specific and informed agreement to the processing of their PII.

[SOURCE: ISO 29100]

Consent Receipt

A record of a consent interaction (or consent record summary linked to the record of consent) provided by a PII Principal to a PII Controller to collect, use and disclose the PII Principal's PII in accordance with an agreed set of terms.

Consent Timestamp

The time and date when consent was obtained from the PII Principal.

Consent Type

The type of the consent used by the PII Controller as their authority to collect, use or disclose PII.

Explicit (Expressed) Consent

The PII Principal has an opportunity to provide a specific indication that they consent to the collection of their PII for purposes that have been specified in a prior notice or are provided at the time of collection.

[SOURCE: Europe 5.4.4]

Human-readable

(Of text, data, etc.) in a form that can be naturally or easily read by a person (frequently in contrast to computer-readable, machine-readable).

[SOURCE: OXFORD]

Implicit (Implied) Consent

The PII Controller has a reasonable expectation to believe that consent already exists for the collection of the PII.

Opt-in

A process or type of policy whereby the personally identifiable information (PII) principal is required to take an action to express explicit, prior consent for their PII to be processed for a particular purpose.

[SOURCE: ISO 29100]

Note: If the PII Principal does nothing, consent will not have been obtained.

Opt-out

A process or type of policy whereby the PII principal is required to take a separate action in order to withhold or withdraw consent, or oppose a specific type of processing.

[SOURCE: ISO 29100]

Note: If the PII Principal does nothing, consent will have been deemed to have been obtained.

Privacy Statement

A notice published or provided by the PII Controller to inform the PII Principal of what will be done with their information.

Note: The contents of this notice may be required by regulation and may include information that is beyond the scope of this specification.

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.

NOTE: To determine whether or not an individual should be considered identifiable, several factors need to be taken into account.

[SOURCE: ISO 29100]

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.

[SOURCE: ISO 29100]

Note: may also be called data controller.

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.”

[SOURCE: ISO 29100]

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]

Processing of PII

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

NOTE: Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII.

[SOURCE: ISO 29100]

Privacy Stakeholder

A natural or legal person, public authority, agency or any other body that can affect, be affected by, or perceive themselves to be affected by a decision or activity related to personally identifiable information (PII) processing.

[SOURCE: ISO 29100]

Purpose

1. The business, operational or regulatory requirement for the collection, use and/or disclosure of a PII Principal's data.

2. The reason personal information is collected by the entity.

[SOURCE: GAPP]

Third Party

A privacy stakeholder other than the personally identifiable information (PII) principal, the PII controller and the PII processor, and the natural persons who are authorized to process the data under the direct authority of the PII controller or the PII processor.

[SOURCE: ISO 29100]

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.

NOTE: In some jurisdictions or in specific contexts, sensitive PII is defined in reference to the nature of the PII and can consist of PII revealing the racial origin, political opinions or religious or other beliefs, personal data on health, sex life or criminal convictions, as well as other PII that might be defined as sensitive.

[SOURCE: ISO 29100]

Sensitive Personal Information (SPI) is defined as information that if lost, compromised, or disclosed could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

[SOURCE: DHS HSSPII]

NOTE: For this specification, 'Sensitive data' may be considered synonymous with Sensitive PII. Sensitive Data is defined in Section 2 of the Data Protection Act of the UK (http://www.legislation.gov.uk/ukpga/1998/29/section/2) as personal data consisting of information relating to the data subject concerning racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership; physical or mental health or other data or as defined by implementers of the specification. In the [GDPR], this is referred to as special categories of data.

Use

Any processing of PII done by a PII Controller or by a PII processor on behalf of a PII Controller.

NOTE: "collection, use, and disclosure" is a useful articulation of the steps in PII processing.

4 ELEMENTS OF A CONSENT RECEIPT

4.1 Introduction

The following sub-sections define the fields for a Consent Receipt including the corresponding JSON field names and types. This specification uses “named object” data types to describe the principal concepts within the Consent Receipt and allows for extension by implementers. See the JSON schema for object implementation.

4.2 Conformance

A Consent Receipt MUST include the fields defined as REQUIRED below. When using JSON, the Consent Receipt MUST also be valid per the Consent Receipt schema in Section 4.8. Additional fields MAY be added as long as they don't conflict with the conformance requirements.

4.3 Consent Receipt Transaction Fields

This section defines the administrative fields for the consent transaction and the metadata for the overall Consent Receipt.

4.3.1 Version

REQUIRED: The version of this specification to which a receipt conforms. The value MUST be “KI-CR-v1.1.0” for this version of the specification.

JSON: `version`, type: `string`

4.3.2 Jurisdiction

REQUIRED: The jurisdiction(s) applicable to this transaction. This field MUST contain a non-empty string describing the jurisdiction(s).

JSON: `jurisdiction`, type: `string`

4.3.3 Consent Timestamp

REQUIRED: Date and time of the consent transaction. 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.

JSON: `consentTimestamp`, type: `integer`

4.3.4 Collection Method

REQUIRED: A description of the method by which consent was obtained. Collection Method is a key field for context and determining what fields MUST be used for the Consent Receipt. This field MUST contain a non-empty string.

JSON: `collectionMethod`, type: `string`

4.3.5 Consent Receipt ID

REQUIRED: A unique number for each Consent Receipt. SHOULD use UUID-4 [RFC 4122]. This field MUST contain a non-empty string.

JSON: `consentReceiptID`, type: `string`

4.3.6 Public Key

OPTIONAL: The PII Controller's public key.

JSON: `publicKey`, type: `string`

4.3.7 Language

OPTIONAL: Language in which the consent was obtained. MUST use ISO 639-1:2002 [ISO 639] if this field is used.

JSON: `language`, type: `string`

4.4 Consent Transaction Parties Fields

This section defines information about the parties involved in the consent process.

4.4.1 PII Principal ID

REQUIRED: PII Principal-provided identifier. E.g., email address, claim, defined/namespace. Consent is not possible without an identifier. This field MUST contain a non-empty string.

JSON: `piiPrincipalId`, type: `string`

4.4.2 piiControllers

REQUIRED: An array that contains one or more items where each item represents one PII Controller. It is only required for the JSON encoding of a Consent Receipt.

JSON: `piiControllers`, type: `array`

4.4.3 PII Controller

REQUIRED: Name of the first PII Controller who collects the data. This entity is accountable for compliance with the management of PII. The PII Controller determines the purpose(s) and type(s) of PII processing. There may be more than one PII Controller for the same set(s) of operations performed on the PII, in which case the different PII Controllers SHOULD be listed. For Sensitive PII, the PII Controller MUST be specified with legally required explicit notice to the PII Principal. This field MUST contain a non-empty string.

JSON: `piiController`, type: `string`

4.4.4 On Behalf

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.

JSON: `onBehalf`, type: `boolean`

4.4.5 PII Controller Contact

REQUIRED: Contact name of the PII Controller. This field MUST contain a non-empty string.

JSON: `contact`, type: `string`

4.4.6 PII Controller Address

REQUIRED: The physical address of PII controller. Postal address for contacting the PII Controller. The JSON value MUST follow the schema at https://schema.org/PostalAddress.

JSON: `address`, type: `object`

4.4.7 PII Controller Email

REQUIRED: Contact email address of the PII Controller. The direct email to contact the PII Controller regarding the consent or privacy contract. This field MUST contain a non-empty string.

JSON: `email`, type: `string`

4.4.8 PII Controller Phone

REQUIRED: Contact phone number of the PII Controller. The business phone number to contact the PII Controller regarding the consent. This field MUST follow RFC 3966 [RFC 5341].

JSON: `phone`, type: `string`

4.4.9 PII Controller URL

OPTIONAL: A URL for contacting the PII Controller.

JSON: `piiControllerURL`, type: `string`

4.4.10 Privacy Policy

REQUIRED: A link to the PII Controller's privacy statement/policy and applicable terms of use in effect when the consent was obtained, and the receipt was issued. If a privacy policy changes, the link SHOULD continue to point to the old policy until there is evidence of an updated consent from the PII Principal. This field MUST contain a non-empty string.

JSON: `policyURL`, type: `string`

4.5 Data, Collection, and Use Fields

This section defines the fields for services, personal information categories, attributes, PII, and PII Sensitivity.

4.5.1 services

REQUIRED: An array that contains one or more items where each item represents one Service. It is only required for the JSON encoding of a Consent Receipt.

JSON: `services`, type: `array`

4.5.2 Service

REQUIRED: The service or group of services being provided for which PII is collected. The name of the service for which consent for the collection, use, and disclosure of PII is being provided. This field MUST contain a non-empty string.

JSON: `service`, type: `string`

4.5.3 purposes

REQUIRED: An array that contains one or more items where each item represents one Purpose. It is only required for the JSON encoding of a Consent Receipt.

JSON: `purposes`, type: `array`

4.5.4 Purpose

OPTIONAL: A short, clear explanation of why the PII is required.

JSON: `purpose`, type: `string`

4.5.5 Purpose Category

REQUIRED: The reason the PII Controller is collecting the PII. Example Purpose Categories currently in use are available on the Kantara Consent & Information Sharing Work Group (CISWG) Wiki page (https://kantarainitiative.org/confluence/x/74K-BQ). This field MUST contain a non-empty string.

JSON: `purposeCategory`, type: `string`

4.5.6 Consent Type

REQUIRED: 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”. If consent was not explicit, a description of the consent method MUST be provided. This field MUST contain a non-empty string.

JSON: `consentType`, type: `string`

4.5.7 PII Categories

REQUIRED: A list of defined PII categories. PII Category should reflect the category that will be shared as understood by the PII Principal. More information can be found on the Kantara Consent & Information Sharing Work Group (CISWG) Wiki page. (https://kantarainitiative.org/confluence/x/74K-BQ). This field MUST contain a non-empty string.

JSON: `piiCategory`, type: `array`

4.5.8 Primary Purpose

OPTIONAL: Indicates if a purpose is part of the core service of the PII Controller. Possible values are TRUE or FALSE.

JSON: `primaryPurpose`, type: `boolean`

4.5.9 Termination

REQUIRED: Conditions for the termination of consent. Link to policy defining how consent or purpose is terminated. This field MUST contain a non-empty string.

JSON: `termination`, type: `string`

4.5.10 Third Party Disclosure

REQUIRED: Indicates if the PII Controller is disclosing PII to a third party. Possible values are TRUE or FALSE.

JSON: `thirdPartyDisclosure`, type: `boolean`

4.5.11 Third Party Name

REQUIRED: The name or names of the third party to which the PII Processor may disclose the PII. MUST be supplied if Third Party Disclosure is TRUE and MUST contain a non-empty string.

JSON: `thirdPartyName`, type: `string`

4.5.12 Sensitive PII

REQUIRED: Indicates whether the consent interaction contains PII that is designated sensitive or not sensitive. Possible values are TRUE or FALSE. A value of TRUE indicates that data covered by the Consent Receipt is sensitive, or could be interpreted as sensitive, which indicates that there is policy information out-of-band of the Consent Receipt.

JSON: `sensitive`, type: `boolean`

4.5.13 Sensitive PII Category

REQUIRED: A listing of categories where PII data collected is sensitive. The field MUST contain a non-empty string if Sensitive PII is TRUE.

JSON: `spiCat`, type: `array`

4.6 Consent Receipt data structure

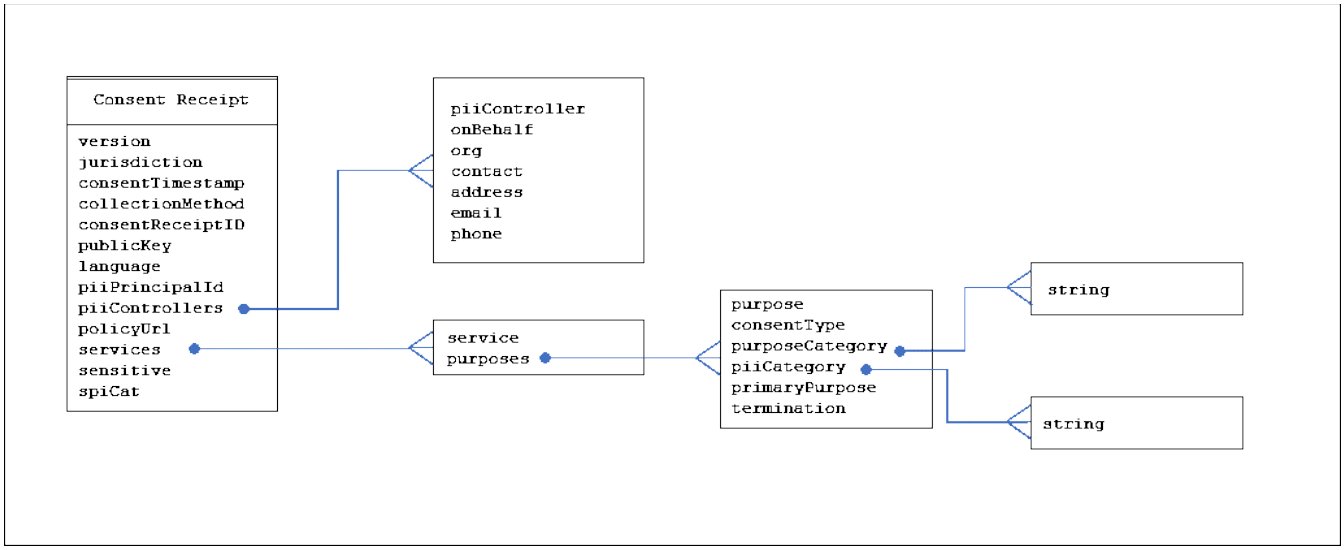

Figure 1

4.7 Presentation and Delivery

Although a CR can be provisioned in any manner that is feasible or expected based on the context, a CR MUST be provided to the PII Principal in a human-readable format either on screen or delivered to the PII Principal, or both. A JSON encoded CR MAY also be delivered to the PII Principal.

441 We note that in some use cases, the PII Controller may primarily depend upon a proprietary
442 consent management system that may display a receipt on demand. So long as the
443 presentation UI contains the information set out in this standard, it will be deemed to be a
444 human-readable Consent Receipt.

445 NOTE: Issues such as language translation, localization, human-readable layout and
446 formatting, and delivery mechanisms are out-of-scope for this document.

447

4.8 JSON Schema

```
{
   // Kantara Consent Receipt Specification v 1.1.0 DRAFT 6
   //2017-11-17

  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "version": {
      "type": "string"
    },
    "jurisdiction": {
      "type": "string"
    },
    "consentTimestamp": {
      "type": "integer",
      "minimum" : 0
    },
    "collectionMethod": {
      "type": "string"
    },
    "consentReceiptID": {
      "type": "string"
    },
    "publicKey": {
      "type": "string"
    },
    "language": {
      "type": "string"
    },
    "piiPrincipalId": {
      "type": "string"
    },
    "piiControllers": {
        "type": "array",
            "items": {
              "type": "object",
              "properties": {
                "piiController": {
                  "type": "string"
                },
                "onBehalf": {
                  "type": "boolean"
                },
                "contact": {
                  "type": "string"
                },
                "address": {
                  "type": "object"
                },
                "email": {
                  "type": "string"
                },
                "phone": {
                  "type": "string"
                },
                "piiControllerUrl": {
                  "type": "string"
                }
              },
              "required": [
                "piiController",
```

```
              "contact",
              "address",
              "email",
              "phone"
            ]
          }
      },
  "policyUrl": {
    "type": "string"
  },
  "services": {
    "type": "array",
    "items": {
      "type": "object",
      "properties": {
        "service": {
          "type": "string"
        },
        "purposes": {
          "type": "array",
          "items": {
            "type": "object",
            "properties": {
              "purpose": {
                "type": "string"
              },
              "consentType": {
                "type": "string"
              },
              "purposeCategory": {
                "type": "array",
                "items": {
                  "type": "string"
                }
              },
              "piiCategory": {
                "type": "array",
                "items": {
                  "type": "string"
                }
              },
              "primaryPurpose": {
                "type": "boolean"
              },
              "termination": {
                "type": "string"
              }
            },
            "oneOf": [
              {
                "properties": {
                  "thirdPartyDisclosure": {
                    "type": "boolean",
                    "enum": [
                      false
                    ]
                  }
                },
                "required": [
                  "thirdPartyDisclosure"
                ]
              },
              {
                "properties": {
```

```
                    "thirdPartyDisclosure": {
                      "type": "boolean",
                      "enum": [
                        true
                      ]
                    },
                    "thirdPartyName": {
                      "type": "string"
                    }
                  },
                  "required": [
                    "thirdPartyDisclosure",
                    "thirdPartyName"
                  ]
                }
              ],
              "required": [
                "consentType",
                "purposeCategory",
                "piiCategory",
                "termination",
                "thirdPartyDisclosure"
              ]
            }
          }
        },
        "required": [
          "service",
          "purposes"
        ]
      }
    },
    "sensitive": {
      "type": "boolean"
    },
    "spiCat": {
      "type": "array",
      "items": {
        "type": "string"
      }
    }
  },
  "required": [
    "version",
    "jurisdiction",
    "consentTimestamp",
    "collectionMethod",
    "consentReceiptID",
    "piiPrincipalId",
    "piiControllers",
    "services",
    "policyUrl",
    "sensitive",
    "spiCat"
  ]
}
```

5 CONSIDERATIONS

5.1 General

Consent is a means for people to regulate their privacy in a specific context. As a social control, consent is a signal people provide when they share personal information specific to that context. Since the scope of each context will vary, different Consent Receipt implementations will have different requirements for user experience, legal, privacy, and security-related considerations for the collection disclosure and use of PII consent by the PII Controller.

5.2 Sensitive PII

In some jurisdictions there are categories listed as sensitive personal information. If the use, collection or disclosure of sensitive personal information has legal requirements as defined in regulation, explicit consent is probably required with jurisdiction-specific legal notice requirements. For example, PII revealing the racial origin, political opinions or religious or other beliefs, personal data on health, sex life or criminal convictions, as well as other PII that are defined as sensitive in regulation.

5.3 Security and Integrity

5.3.1 Overview

Since Consent Receipts can contain PII, it is a requirement that transmission of Consent Receipts does not take place in the clear and that secure communications be used, e.g., HTTPS. The requirements for implementers of Consent Receipts and consent management solutions include signing, encryption, key management and other operations for their creation, transmission, use, and storage if the Consent Receipt is to be used for proof of consent, withdrawal of consent or any other rights.

5.3.2 Guidance

1. Ensure the use of securely authenticated connections using modern cryptology.
2. If a receipt contains PII - a receipt without PII is not in scope here - and it is transmitted securely, the user must be able to manage the receipt interactions with:
    a. Storage (local machine, server, client, application, device, etc.)
    b. Other receipt repositories and consent services.
        i. Security of these repositories and services - i.e., non-local, requires considerations but is currently out-of-scope of this specification.
        ii. When considered it should include the use case where for some reason a receipt has not been transmitted it should be available from the provider of the receipt repository for direct download. Such infrastructure is out-of-scope for this specification.
    c. Transmission of receipts with PII.
3. The ability to validate and revoke the receipt – and other aspects of the Consent Receipt lifecycle are out-of-scope for this specification at this time but will need to be taken up shortly. Additional topics for future consideration include:
    a. Consent best practices.
    b. Status and revocation of consent.
    c. Consent management, validation, and other aspects of its lifecycle.

672 The transmission of a JSON Consent Receipt should use the following specifications:

673 JSON Web Token (JWT) [RFC 7519]

674 JSON Web Encryption (JWE) [RFC 7516]

675 JSON Web Signature (JWS) [RFC 7515]

6 ACKNOWLEDGEMENTS

The Consent Receipt effort has been developed in the Kantara Community, supported by people who have invested in making this specification open and free to use. It is free so that people can have a common way to see what consents have been provided and what data is being shared or disclosed. If you wish to provide feedback, you may join the Kantara Working Group, and then email us on our list at wg-infosharing@kantarainitiative.org or send feedback to staff@kantarainitiative.org .

In addition to Kantara, we wish to thank the following contributors to the Consent Receipt effort:

Customer Commons

Colin Wallis

Justin Richer

Sarah Squire

Eve Maler

Joss Langford

Thomas Lenggenhager

Tom Jones

Barry Hieb

The Consent Receipt standardization effort has been developed with the support of many communities, as noted in our acknowledgments section, and leverages best of breed standards, legal regulation and technical practices in its design and development, as noted in the references section.

7 REFERENCES

[DHS HSSPII] *DHS Handbook for Safeguarding Sensitive PII*. (Ed. 2012). https://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf

[EU-DATA] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

[Europe 5.4.4] Kosta, E., *Consent in European Data Protection Law*. Section 5.4: "Consent in the Context of Sensitive Data." (Ed: 2013) p. 98-100. https://goo.gl/JGPX2Y

[GAPP] *Generally Accepted Privacy Principles* - developed through joint consultation with the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA) through the AICPA/CICA Privacy Task Force. https://www.cippguide.org/2010/07/01/generally-accepted-privacy-principles-gapp/

[GDPR] *General Data Protection Regulation*, http://www.eugdpr.org/article-summaries.html

[ISO 639] ISO 639-1:2002, *Codes for the representation of names of languages — Part 1: Alpha-2 code* https://www.iso.org/standard/22109.html

[ISO 18001-1:2005] *Information technology — Personal identification — ISO-compliant driving license — Part 1: Physical characteristics and basic data set.* https://www.iso.org/obp/ui/#iso:std:iso-iec:18013:-1:ed-1:v1:en

[ISO 29100:2011] *Information technology -- Security techniques -- Privacy framework.* http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123

[PIPEDA] *Personal Information Protection and Electronic Documents Act*, http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

[RFC 2119] Bradner, S., "*Key words for use in RFCs to Indicate Requirement Levels*", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997 http://www.rfc-editor.org/info/rfc2119

[RFC 5341] C. Jennings, V. Gurbani, "The Internet Assigned Number Authority (IANA) tel Uniform Resource Identifier (URI) Parameter Registry", RFC 5341, DOI: 10.17487/RFC5341, September 2008, https://tools.ietf.org/html/rfc5341

[RFC 4122] P. Leach, M. Mealling, R. Salz, "*A Universally Unique IDentifier (UUID) URN Namespace*", RFC 4122, 10.17487/RFC4122, July 2005, https://tools.ietf.org/html/rfc4122

[RFC 7159] Bray, T., Ed., "*The JavaScript Object Notation (JSON) Data Interchange Format*", RFC 7159, DOI 10.17487/RFC7159, March 2014, http://www.rfc-editor.org/info/rfc7159

[RFC 7515] M. Jones, J. Bradley, N. Sakimura, "*JSON Web Signature (JWS)*", RFC 7515, May 2015, https://tools.ietf.org/html/rfc7515

[RFC 7516] M. Jones, J. Hildebrand, "*JSON Web Encryption (JWE)*", RFC 7516, May 2015, https://tools.ietf.org/html/rfc7516

[RFC 7519] M. Jones, J. Bradley, N. Sakimura, "*JSON Web Token (JWT)*", RFC 7519, DOI 10.17487/RFC7519, May 2015, https://tools.ietf.org/html/rfc7519

738 **[OECD]** *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal*
739 *Data*.
740 http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflo
741 wsofpersonaldata.htm

742 **[OXFORD]** Oxford University Press - Definition of human-readable in English,
743 https://en.oxforddictionaries.com/definition/us/human-readable

APPENDIX A: EXAMPLE CONSENT RECEIPTS

A.1 Human-readable Consent Receipt – Simple

Consent Receipt[1]	
Version	KI-CR-v1.1.0
Jurisdiction	Discworld
Consent Timestamp	11/13/2017, 12:00:00 PM EST
Collection Method	Web Subscription Form with opt-in for marketing
Consent Receipt ID	c1befd3e-b7e5-4ea6-8688-e9a565aade21
Public Key	04:a3:1d:40:53:f0:4b:f1:f9:1b:b2:3a:83:a9:d1: 40:02:cc:31:b6:4a:77:bf:5e:a0:db:4f:ea:d2:07: c4:23:57:6f:83:2c:3d:3e:8d:e7:02:71:60:54:01: f4:6a:fb:a2:1e:8b:42:53:33:78:68:d9:7d:5e:b2: cc:0b:f8:a1:bf
Language	English
Consent Parties	
Information Subject	
PII Principle ID	**Bowden Jeffries**
Information Controller	
PII Controller Name	**Ankh-Morpork Times**
PII Controller Contact	William de Word, Chief Editor & Data Protection Officer
PII Controller Address	Ankh-Morpork Times Gleam Street, Ankh-Morpork, Discworld
PII Controller Email	william@times.ankh-morpork.xyz
PII Controller Phone	(555) 555-DISC (3429)
PII Controller URL	https://www.times.ankh-morpork.xyz/contact
Privacy Policy	https://times.ankh-morpork.xzy/privacy_2017

Please see the next page for details on the data we have collected about you, and what we will do with it.

[1] Sample Consent Receipt, version 1.1.0

Data, collection and use				
Service	**Digital Subscription and News Alerts**			
Purposes for collection and use				
Purpose	*Purpose Category*	*Consent Type*	*PII Categories*	*Primary purpose?*
Fulfil Digital Subscription	Provision of services	EXPLICIT	• Technical • Demographics • Financial • Contact	TRUE
Marketing	Marketing	EXPLICIT	• Demographics • Financial • Contact	FALSE
Financial Record Keeping	Fiduciary obligation	N/A	• Financial	FALSE
Law Enforcement	Legal obligation	N/A	• All	FALSE
Termination	https://times.ankh-morpork.xzy/privacy_2017#termination			
Third Party Disclosure	**True**			
Third Party Names	• Outsourced printer • Outsourced fulfillment vendor • Bank • Law enforcement with subpoena • Digital Advertising Agency			
Sensitive PII	**Yes**			
Sensitive PII Category	**Financial Information**			

748
749

A.2 Human-readable Consent Receipt – Fancy

Receipt for Personally Identifiable Information

Service: Digital Subscription and News Alerts

At the Ankh-Morpork Times we take your privacy seriously. This document is being provided to you as a receipt for personally identifiable information that we have, or will collect about you. It tells you what information has been collected and for what purposes we will use and disclose it. For your information, this document is based on the Consent Receipt Specification v1.1.0 published by the Kantara Initiative.

We have collected, or will collect, the information described below based on your implicit consent when you completed our web subscription form. If you receive marketing material, it will because you ticked an opt-in check box for marketing. We operate and follow the data protection rules for DiscWorld (dw). We will continue to collect and use your information until 1 year after your subscription ends.

YOUR ID: BOWDEN JEFFRIES

Types of Information we have or may collect about you[s].	The purposes for collection of your personal information[on].
General biographical information about you (demographics) Your financial information for payments [s] Your contact information	Technical data for web servers (Core Function) News web site and alerts (Contracted Service) Marketing [o] Meeting Fiduciary & Legal Obligations[n]

About Us: The Ankh-Morpork Times is the Personally Identifiable Information Controller that is accountable for the information that has been collected about you. We are acting on our own behalf. For more details on our privacy notice and practices see the privacy policy linked to below.

Our Contact Information	The Ankh-Morpork Times Gleam Street, Ankh-Morkpork, Discworld https://www.times.ankh-morpork.xyz/contact
Privacy Contact	William de Worde, Chief Editor and Privacy Officer william@times.ankh-morpork.xyz (555) 555-DISC (3429) x 7748229 (Privacy)
Privacy Policy	https://times.ankh-morpork.xzy/privacy_2017

Third parties how may receive information about you:

Outsourced printer	Bank	Digital Advertising Agency
Outsourced fulfillment vendor	Law enforcement with subpoena	

Receipt #: c1befd3e-b7e5-4ea6-8688-e9a565aade21
Date: 11/13/2017, 12:00:00 PM EST

[s] Information marked with a superscript s may be treated as "Sensitive Personal Information"
[o] Purposes marked with a superscript o indicated an optional consent.
[n] Purposes marked with a superscript n do not require consent

A.3 JSON Consent Receipt

```
{
  "version": "KI-CR-v1.1.0",
  "jurisdiction": "DW",
  "consentTimestamp": 1510592400,
  "collectionMethod": "Web Subscription Form with opt-in for marketing",
  "consentReceiptID": "c1befd3e-b7e5-4ea6-8688-e9a565aade21",
  "publicKey":
"04:a3:1d:40:53:f0:4b:f1:f9:1b:b2:3a:83:a9:d1:\r\n40:02:cc:31:b6:4a:77:bf:5
e:a0:db:4f:ea:d2:07:\r\nc4:23:57:6f:83:2c:3d:3e:8d:e7:02:71:60:54:01:\r\nf4
:6a:fb:a2:1e:8b:42:53:33:78:68:d9:7d:5e:b2:\r\ncc:0b:f8:a1:bf",
  "language": "en",
  "piiPrincipalId": "Bowden Jeffries",
  "piiControllers": [
    {
      "piiController": "Ankh-Morpork Times",
      "contact": "William De Worde",
      "address": {
        "streetAddress": "Gleam Street",
        "addressCountry": "DW"
      },
      "email": "william@times.ankh-morpork.xyz",
      "phone": "(555) 555-DISC (3429)"
    }
  ],
  "policyUrl": "https://times.ankh-morpork.xzy/privacy_2017",
  "services": [
    {
      "service": "Digital Subscription and News Alerts",
      "purposes": [
        {
          "purpose": "To provide contracted services",
          "purposeCategory": [
            "2 - Contracted Service"
          ],
          "consentType": "EXPLICIT",
          "piiCategory": [
            "1 - Biographical",
            "2 - Contact",
            "4 - Communications/Social",
            "7 - Financial"
          ],
          "primaryPurpose": true,
          "termination": "Subscription end date + 1 year",
          "thirdPartyDisclosure": true,
          "thirdPartyName": "The Ankh-morpork Deadbeat Debt Collectors
Society"
        },
        {
          "purpose": "To personalize service experience",
          "purposeCategory": [
            "5 - Personalize Experience"
          ],
          "consentType": "EXPLICIT",
          "piiCategory": [
            "1 - Biographical",
            "2 - Contact",
            "4 - Communications/Social"
          ],
          "primaryPurpose": false,
          "termination": "Subscription end date + 1 year",
          "thirdPartyDisclosure": false
```

```
        },
        {
          "purpose": "To market services",
          "purposeCategory": [
            "6 - Marketing"
          ],
          "consentType": "EXPLICIT",
          "piiCategory": [
            "2 - Contact"
          ],
          "primaryPurpose": false,
          "termination": "Subscription end date + 1 year",
          "thirdPartyDisclosure": false,
          "thirdPartyName": "DiscWorld Octarine Programmatic Ad Agency"
        },
        {
          "purpose": "Complying with legal obligations",
          "purposeCategory": [
            "12 - Legally Required Data Retention",
            "13 - Required by Law Enforcement or Government"
          ],
          "consentType": "N/A",
          "piiCategory": [
            "1 - Biographical",
            "2 - Contact",
            "4 - Communications/Social",
            "7 - Financial"
          ],
          "primaryPurpose": false,
          "termination": "N/A",
          "thirdPartyDisclosure": true,
          "thirdPartyName": "Requesting legal authority"
        }
      ]
    }
  ],
  "sensitive": true,
  "spiCat": [
    "1 - Biographical",
    "7 - Financial"
  ]
}
```

857

REVISION HISTORY

Version	Date	Summary of Substantive Changes
1.1.0 DRAFT 1	2017-02-28	Initial v1.1 draft
1.1.0 DRAFT 2	2017-07-12	Sprint 2 draft.
1.1.0 DRAFT 3	2017-08-23	Sprint 3 draft
1.1.0 DRAFT 4	2017-10-19	Roll up of Sprint 4 – Sprint 6
1.1.0 DRAFT 5	2017-10-25	Major reorg of document.
1.1.0 DRAFT 6	2017-11-17	Final revisions and updates to the document.
1.1.0 DRAFT 7	2017-11-20	Additional clean-up
1.1.0 DRAFT 8	2018-02-15	Revisions based on comment from public review period.
1.1.0	2018-05-02	Candidate Kantara Initiative Technical Specification Recommendation
1.1.0	2018-05-25	Final Recommendation approved by Kantara All-Member Ballot

858

859