Consent Receipt Specification

Version: 1.0.0 DRAFT 2

Date: 2016-12-16

Editor: Mark Lizar, David Turner

Contributors: Iain Henderson, Mary Hodder, Harri Honko, Oliver Maerz, Eve Maler, John Wunderlich

Status: Kantara Initiative Candidate Recommendation Draft

Abstract:

A Consent Receipt is a record of consent used by a PII Controller as their authority to collect, use and disclose a PII Principal's personally identifiable information (PII). The Consent Receipt will be provided to the PII Principal that gave the consent. This specification defines the requirements for a receipt given to the PII Principal. The receipt includes links to existing privacy notices & policies as well as a description of what information will be collected, the purposes for that collection and 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:

Notice:

Table of Contents

Abstract: 1

1 Introduction 3

2 Notations and Abbreviations 4

3 Terms and definitions 5

4 Consent Receipt 9

4.1 Contents of receipt 9

4.2 Presentation and Delivery 11

5 Consent Receipt - JSON 12

5.1 JSON Fields 12

5.2 JSON Schema 14

6 Conformance 17

7 Considerations 19

7.1 A Consent Receipt is PII 19

7.2 Sensitive PII: Liability & Compliance 19

7.3 Formatting JSON as JWT 20

8 Acknowledgements 21

9 References 22

Appendix A: PII Categories of Data 23

Appendix B: Example Consent Receipts 25

Revision history 29

1 INTRODUCTION

Current best practices and regulations for privacy protection, and privacy by design, set out requirements for notice and consent, however, there is no standard or specification for recording consent. As a result, individuals cannot easily track their consents or monitor how their information is processed or know who to hold accountable in the event of a breach of their privacy.

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 an individual agreeing to allow an organization to collect, use, and/or disclose their data, and data about them, according to a set of terms and conditions defined by the organization. At present, individuals do not have an easy way to manage the consent they have given, how information about them is processed, or a means to hold organizations accountable for violations of consent.

A record of a consent transaction 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 transaction and give it to the individual, defined here as a Consent Receipt. 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 consent receipt elements described in this specification represent privacy-related requirements common to many jurisdictions. A JavaScript Object Notation (JSON) schema for a consent receipt 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.

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.
https://docs.kantarainitiative.org/uma/rec-uma-core.html# - RFC7159

CPO	Chief Privacy Officer
CR	Consent Receipt
DPO	Data Protection Officer
JSON	JavaScript Object Notation
JWT	JSON Web Token
GDPR	General Data Protection Regulation
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"* and other published, recognized efforts to maintain consistency with the terms commonly used in the ecosystem. If other organizations' terms are not compatible with this specification, this document will define those terms for clarity and specificity for our purposes.

3.1 Collection

Receiving or obtaining data from or about a natural person.

3.2 Disclosure

The transfer or copy, by a PII Controller or a PII Processor acting on their behalf, of PII and accountability for that PII 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 PII Principal, both this 'use' and actual 'disclosure' may be termed 'sharing' information. However, these are significant differences from a transparency and regulatory point of view.

3.3 Consent

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

[SOURCE: ISO 29100]

3.4 Consent Receipt

A record of the 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.

3.5 Consent Timestamp

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

3.6 Consent Type

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

3.7 Explicit (Expressed) Consent

The user 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.

[Europe 5.4.4]

3.8 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]

3.9 Implicit (Implied) Consent

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

3.10 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 user does nothing, consent will not have been obtained.

3.11 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 user does nothing, consent will have been deemed to have been obtained.

3.12 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.

3.13 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]

3.14 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]

3.15 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]

3.16 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]

3.17 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]

3.18 Purpose

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

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

[SOURCE: GAPP]

3.19 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]

3.20 Sensitive PII

Sensitive Categories of personal information, 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 those related 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.

3.21 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 CONSENT RECEIPT

4.1 Contents of receipt

Consent Receipt Transaction Details Administrative fields for the consent transaction and the metadata for the overall Consent Receipt.		
Field Name	**Definition**	**Guidance**
Version	The version of this specification a receipt conforms to.	The value MUST be “KI-CR-v1.0.0” for this version of the specification.
Jurisdiction	Jurisdiction(s) applicable to this transaction.	This field MUST contain a non-empty string describing the jurisdiction(s).
Consent Timestamp	Date and time of the consent transaction	MUST include a time zone or indicate UTC. Presentation to end users SHOULD consider localization requirements.
Collection Method	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.
Consent Receipt ID	A unique number for each Consent Receipt.	For example, UUID-4 [RFC 4122]
Public Key	The PII Controller’s public key used to sign the consent receipt.	
Consent Transaction Parties		
Field Name	**Definition**	**Guidance**
PII Principal ID	PII Principal provided identifier. E.g. email address, claim, defined/namespace.	Consent is not possible without an identifier.
PII Controller	Name of the initial PII controller who collects the data. This entity is accountable for compliance over 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 this case, the different PII Controllers SHOULD be listed, and it MUST be listed for Sensitive PII with legally required explicit notice to the PII Principal.
On Behalf	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.

PII Controller Address	The physical address of PII controller.	Address for contacting the DPO in writing.
PII Controller Contact	Contact name of the PII Controller	Name and/or title of the DPO.
PII Controller Email	Contact email address of the PII Controller	The direct email to contact the PII Controller regarding the consent. e.g., DPO, CPO, privacy contact.
PII Controller Phone	Contact phone number of the PII Controller.	The business phone number to contact the PII Controller regarding the consent. e.g., DPO, CPO, administrator.
Data, collection, and use This section specifies services, personal information categories, attributes, PII confidentiality level, and PII Sensitivity.		
Field Name	**Definition**	**Guidance**
Privacy Policy	A link to the privacy 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.
Service	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.
Purpose	A short, clear explanation of why the PII item is required.	This field MUST contain a non-empty string.
Purpose Category	The reason the PII Controller is collecting the PII.	Example Purpose Categories currently in use can are available on the Kantara Consent & Information Sharing Work Group (CISWG) Wiki page (http://kantarainitiative.org/confluence/display/infosharing/Appendix+CR+-+V.9.3+-+Example+Purpose+Categories)
Consent Type	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.
PII Categories	A list of defined PII categories.	PII Category should reflect the category that will be shared as understood by the PII Principal. In Appendix B there is an example of a defined list as supplied by a PII

		Controller.
Primary Purpose	Indicates if a purpose is part of the core service of the PII Controller.	Possible values are TRUE or FALSE. Yes and No can be used when presenting the CR in a human-readable format.
Termination	Conditions for the termination of consent .	Link to policy defining how consent or purpose is terminated.
Third Party Disclosure	Indicates if the PII Controller is disclosing PII to a third party.	Possible values are TRUE or FALSE. Yes and No can be used when presenting the CR in a human-readable format.
Third Party Name	The name or names of the third party the PII Processor may disclose the PII to.	SHOULD be supplied if Third Party Disclosure IS TRUE.
Sensitive PII	Indicates whether PII is 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. Yes and No can be used when presenting the CR in a human-readable format.
Sensitive PII Category	Listing the categories where PII data collected is sensitive.	The field MUST contain a non-empty string if Sensitive PII is TRUE. See section 7.2 for common sensitive PII categories that have specific consent notice requirements

4.2 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.

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

5 CONSENT RECEIPT - JSON

5.1 JSON Fields

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.

JSON name	CR name	Data Type	Format/Example
version	Version	string	
jurisdiction	Jurisdiction	string	
consentTimestamp	Consent Timestamp	integer	number of seconds since 1970-01-01 00:00:00 GMT
collectionMethod	Collection Method	string	
consentReceiptID	Consent Receipt ID	string	
publicKey	Public Key	string	
subject	PII Principal ID	string	
dataController		object	
onBehalf	On Behalf	boolean	
org	PII Controller Organization	string	
contact	PII Controller Contact Name	string	
address	PII Controller address	object	https://schema.org/PostalAddress
email	PII Controller email	string	
phone	PII Controller phone	string	

JSON name	CR name	Data Type	Format/Example
`policyUrl`	Privacy Policy	`string`	HTTP URL
`services`		`array of objects`	
`serviceName`	Service Name	`string`	
`purposes`		`array of objects`	
`purpose`	Purpose	`string`	
`purposeCategory`	Purpose Category	`array of strings`	
`consentType`	Consent Type	`string`	
`piiCategory`	PII Categories	`array of strings`	
`primaryPurpose`	Primary Purpose	`boolean`	
`termination`	Termination	`string`	
`thirdPartyDisclosure`	Third Party Disclosure	`boolean`	
`thirdPartyName`	Third Party Name	`string`	
`sensitive`	Sensitive PII	`Boolean`	
`spiCat`	Sensitive PII Category	`array of strings`	

5.2 JSON Schema

```
{
  "$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"
    },
    "subject": {
      "type": "string"
    },
    "dataController": {
      "type": "object",
      "properties": {
        "onBehalf": {
          "type": "boolean"
        },
        "org": {
          "type": "string"
        },
        "contact": {
          "type": "string"
        },
        "address": {
          "type": "object"
        },
        "email": {
          "type": "string"
        },
        "phone": {
          "type": "string"
        }
      },
      "required": [
        "org",
        "contact",
        "address",
        "email",
        "phone"
      ]
    },
    "policyUrl": {
      "type": "string"
    },
    "services": {
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "serviceName": {
            "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": [
          "serviceName",
          "purposes"
        ]
      }
    },
    "sensitive": {
      "type": "boolean"
    },
    "spiCat": {
      "type": "array",
      "items": {
        "type": "string"
      }
    }
  },
  "required": [
    "version",
    "jurisdiction",
    "consentTimestamp",
    "collectionMethod",
    "consentReceiptID",
    "subject",
    "dataController",
    "services",
    "policyUrl",
    "sensitive",
    "spiCat"
  ]
}
```

6 CONFORMANCE

A Consent Receipt MUST include the fields as defined in the table below. When using JSON, the Consent Receipt MUST also be valid according to the Consent Receipt schema in Section 5.2.

CR name	Requirement
Version	MUST
Jurisdiction	MUST
Consent Timestamp	MUST
Collection Method	MUST
Consent Receipt ID	MUST
Public Key	MAY
PII Principal ID	MUST
PII Controller	MUST
On Behalf	MAY
PII Controller Contact Name	MUST
PII Controller address	MUST
PII Controller email	MUST
PII Controller phone	MUST
Privacy Policy	MUST
Service	MUST
Purpose	MAY
Purpose Category	MUST

CR name	Requirement
Consent Type	MUST
PII Categories	MUST
Primary Purpose	MAY
Termination	MUST
Third Party Disclosure	MUST
Third Party Name	MUST if Third Party Disclosure is TRUE
Sensitive PII Level	MUST
Sensitive PII Category	MUST if Sensitive PII Level is TRUE

404

7 CONSIDERATIONS

Consent is how people regulate privacy. As a social control, consent is the signal people provide when they share personal information that is specific to a particular context. When broken down, the nature of consent for human communication and signaling can be observed in different ways: as implicit consent, opt-out consent, and explicit consent.

With each consent policy notice and a Consent Receipt implementation, there are different UX, legal, privacy, and security-related considerations for the collection disclosure and use of PII consent by the organizations.

7.1 A Consent Receipt is PII

A Consent Receipt combines personal information with the agreement for its use for the service provider to provide services. A Consent Receipt links multiple data sources with an identifier, which when identified in a Consent Receipt constitutes PII. In all jurisdictions, consent for Sensitive Personal Information requires explicit consent, which is prescribed and regulated by privacy law.

7.2 Sensitive PII: Liability & Compliance

In this document, sensitive data collection is indicated with Sensitive PII flag and is REQUIRED. If `sensitive=TRUE`, then the Consent Receipt has limited liability for the provider as different jurisdictions have legal requirements for what is classified as sensitive. In addition, the implementer can define what is sensitive, or confidential, in their privacy policy, even if not classified as sensitive in a particular jurisdiction.

If the implementer selects `sensitive=TRUE` because sensitive data is collected, but, does not provide the categories of sensitive personal information with PII Sensitive Category field, then it is assumed that what is sensitive and how it is managed will be found in the privacy policy linked to in the Consent Receipt.

The provision of a Consent Receipt with `sensitive=TRUE` indicates the provider of the receipt is liable for providing the correct collection, use and disclosure notice as required by law in the provisioning jurisdiction. As a result, there are three levels of liability to consider for Consent Receipts by the implementer:

1. Provision of the Consent Receipt for non-sensitive PII (`sensitive=FALSE`)

2. Provision of a sensitive Consent Receipt with compliance claims out of scope of the receipt (`sensitive=TRUE` but no sensitive PII categories are listed)

3.

a. Provision of a sensitive Consent Receipt with the `sensitive=TRUE` and sensitive PII categories are listed. Sensitive PII Categories MUST be listed in the Consent Receipt for the Consent Receipt to be used for a compliance claim. In this manner, the receipt can inherently demonstrate compliance with consent notice requirements for the particular consent.

b. If the Sensitive PII category is not listed in the Consent Receipt, the Consent Receipt MUST NOT be considered transparent enough itself to be a compliance claim.

NOTE: In multiple jurisdictions, there are categories listed as sensitive personal information. If you use, collect or disclose sensitive personal information these have legal requirements, require explicit consent and can have jurisdiction-specific legal notice requirements to be informed. 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 might be defined as sensitive.

7.3 Formatting JSON as JWT

Transmitting the JSON Consent Receipt as a JSON Web Token (JWT) [RFC 7519] allows validation of the integrity and authenticity of the receipt.

8 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 their data control and sharing. 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 info@consentreceipt.org.

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

Customer Commons

Colin Wallis

Sal D’Agostino

Andrew Hughes

Justin Richer

Sarah Squire

Eve Maler

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.

9 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

[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 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 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 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

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

APPENDIX A: PII CATEGORIES OF DATA

(Explainers/Examples)

Note: Some of these categories are also considered Sensitive PII;

- Biographical – (General information like Name, DOB, Family info (mother's maiden name), marital status. Historical data like educational achievement, general employment history.)
- Contact – (Address, Email, Telephone Number, etc.)
- Biometric – (Photos, fingerprints, DNA. General physical characteristics – height, weight, hair color. Racial/ethnic origin or identification - whether self-identified or not)
- Communications/Social – (Email, messages, and phone records – both content and metadata. Friends and contacts data. PII about self or others.)
- Network/Service – (Login ids, usernames, passwords, server log data, IP addresses, cookie-type identifiers)
- Health – (Ailments, treatments, family doctor info. X-rays and other medical scan data)
- Financial – (This includes information such as bank account, credit card data. Income and tax records, financial assets/liabilities, purchase/sale of assets history.)
- Official/Government Identifiers – (This includes any widely recognized identifiers that link to individual people. Examples include National Insurance, ID card, Social Security, passport and driving license numbers, NHS number (UK). Just the numbers rather than data associated with them.)
- Government Services - i.e. Social Services/Welfare – (Welfare and benefits status and history)
- Judicial – (Criminal and police records, including traffic offenses.)
- Property/Asset – (Identifiers of property – license plate numbers, broadcasted device identifiers. Not financial assets. Could include digital assets like eBook and digital music data)
- Employee Personal Information – (Records held about employees/ members/ students) not elsewhere defined. Incl. HR records such as job title, attendance/disciplinary records. Salary - as opposed to income.)

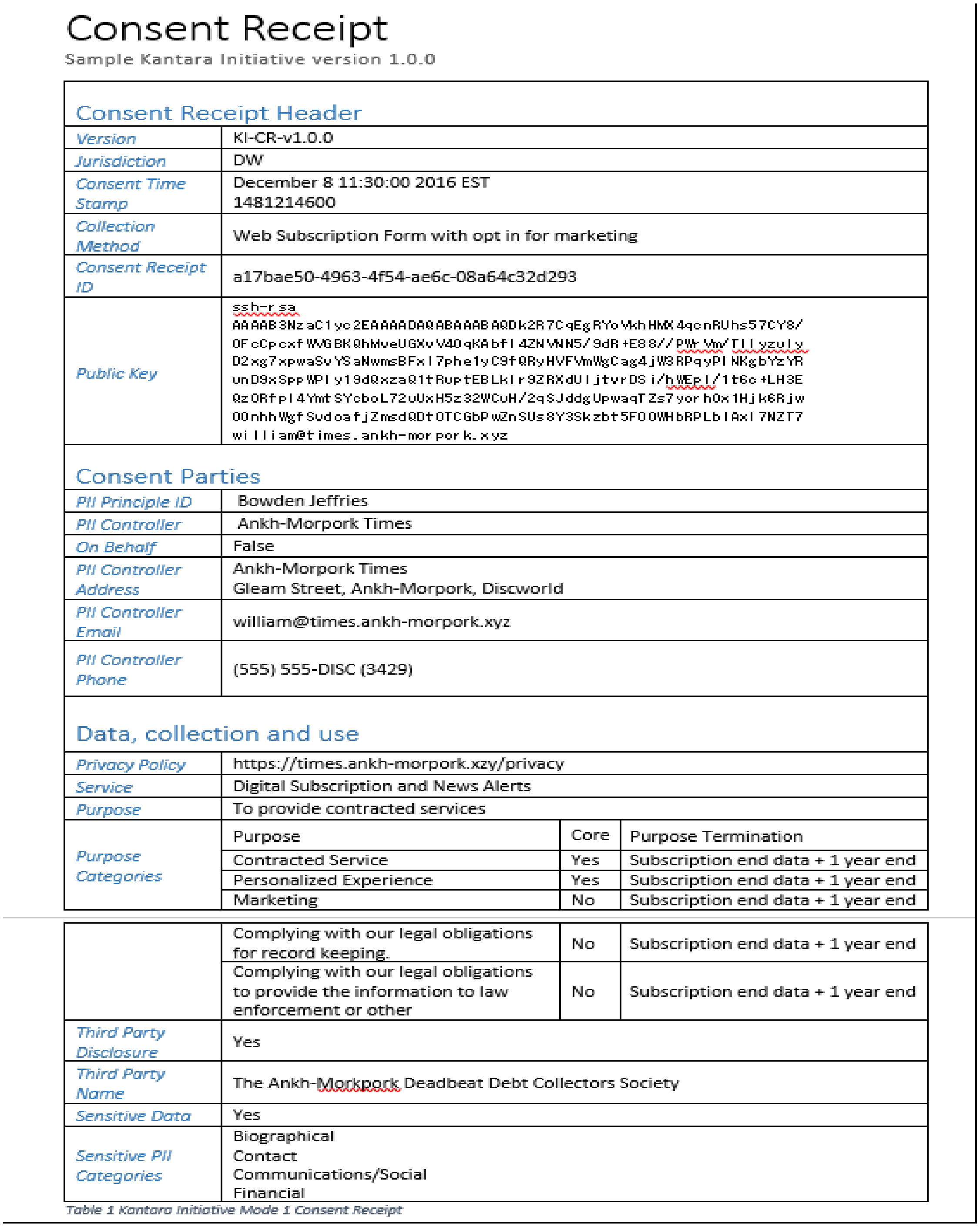
- Psychological/Attitudinal – (Including religious, political beliefs, sexual orientation, and gender identity – though not genetic gender which is Biometric. Traits and personality measures or assessments, but not psychological health - which is health data).

- Membership – (Political, trade union affiliations, any other opt-in organizational/group membership data - third party organizations only. Includes name of the employer when not held by the employer. Could extend to online platform membership. Some might be more sensitive than others – may want a separate category)

- Behavioral – (Any data about the behavior, habits or movements of an individual - electronic or physical. Location, browser/search history, web page usage (analytics), energy usage (smart meters), login history, calendar data, etc.)

543 APPENDIX B: EXAMPLE CONSENT RECEIPTS

544 B.1 Human-readable Consent Receipt – Simple



Consent Receipt

Sample Kantara Initiative version 1.0.0

Consent Receipt Header

Version	KI-CR-v1.0.0
Jurisdiction	DW
Consent Time Stamp	December 8 11:30:00 2016 EST 1481214600
Collection Method	Web Subscription Form with opt in for marketing
Consent Receipt ID	a17bae50-4963-4f54-ae6c-08a64c32d293
Public Key	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDk2R7CqEgRYoVkhHMK4qcnRUhs57CY8/ 0FcCpcxfWVGBKQhMveUGXvV40qKAbfI4ZNVNN5/9dR+E88//PWrVm/TIIyzuIy D2xg7xpwaSvYSaNwmsBFxI7phe1yC9fQRyHVFVmWgCag4jW3RPqyPINKgbYzYR unD9xSppWPIy19dQxzaQ1tRuptEBLkIr9ZRXdUIjtvrDSi/hWEpI/1t6c+LH3E Qz0RfpI4YmtSYcboL72uUxH5z32WCuH/2qSJddgUpwaqTZs7yorh0x1Hjk6Rjw 00nhhWgfSvdoafjZmsdQDtOTCGbPwZnSUs8Y3Skzbt5F00WHbRPLbIAxI7NZT7 william@times.ankh-morpork.xyz

Consent Parties

PII Principle ID	Bowden Jeffries
PII Controller	Ankh-Morpork Times
On Behalf	False
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)

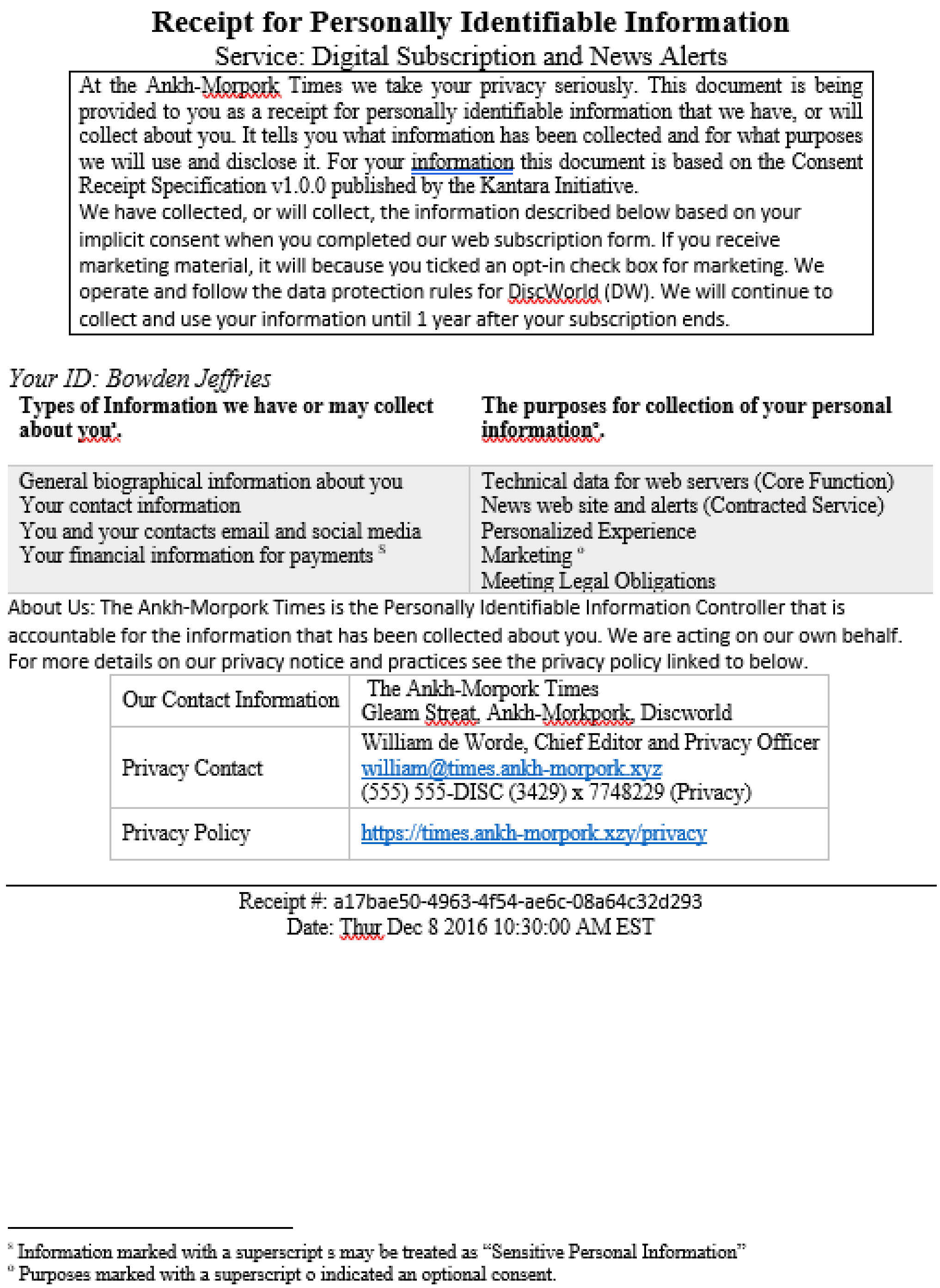
Data, collection and use

Privacy Policy	https://times.ankh-morpork.xzy/privacy		
Service	Digital Subscription and News Alerts		
Purpose	To provide contracted services		
Purpose Categories	Purpose	Core	Purpose Termination
	Contracted Service	Yes	Subscription end data + 1 year end
	Personalized Experience	Yes	Subscription end data + 1 year end
	Marketing	No	Subscription end data + 1 year end
	Complying with our legal obligations for record keeping.	No	Subscription end data + 1 year end
	Complying with our legal obligations to provide the information to law enforcement or other	No	Subscription end data + 1 year end
Third Party Disclosure	Yes		
Third Party Name	The Ankh-Morkpork Deadbeat Debt Collectors Society		
Sensitive Data	Yes		
Sensitive PII Categories	Biographical Contact Communications/Social Financial		

Table 1 Kantara Initiative Mode 1 Consent Receipt

545

B.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 v1.0.0 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[o].**
General biographical information about you	Technical data for web servers (Core Function)
Your contact information	News web site and alerts (Contracted Service)
You and your contacts email and social media	Personalized Experience
Your financial information for payments [s]	Marketing [o]
	Meeting Legal Obligations

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 Streat, Ankh-Morkpork, Discworld
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

Receipt #: a17bae50-4963-4f54-ae6c-08a64c32d293
Date: Thur Dec 8 2016 10:30:00 AM 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.

B.3 JSON Consent Receipt

```
{
  "version": "KI-CR-v1.0.0",
  "jurisdiction": "DW",
  "consentTimestamp": 1481214600,
  "collectionMethod": "Web Subscription Form",
  "consentReceiptID": "a17bae50-4963-4f54-ae6c-08a64c32d293",
  "publicKey": "ss-
rsaAAAAB3NzaC1yc2EAAAADAQABAAABAQDk2R7CqEgRYoVkhHMX4qcnRUhs57CY8OFcCpcxfWVG
BKQhMveUGXvV4OqKAbfI4ZNVNN59dR+E88PWrVmTIIyzuIyD2xg7xpwaSvYSaNwmsBFxl7phe1y
C9fQRyHVFVmWgCag4jW3RPqyPINKgbYzYRunD9xSppWPIy19dQxzaQ1tRuptEBLkIr9ZRXdUljt
vrDSi/hWEpI/1t6c+LH3EQzORfpI4YmtSYcboL72uUxH5z32WCuH/2qSJddgUpwaqTZs7yorh0x
1Hjk6Rjw0OnhhWgfSvdoafjZmsdQDtOTCGbPwZnSUs8Y3Skzbt5F00WHbRPLblAxI7NZT7willi
am@times.ankh-morpork.xyz",
  "subject": "Bowden Jeffries",
  "dataController": {
    "org": "Ankh-Morpork Times",
    "contact": "William De Worde",
    "address": {
      "streetAddress": "Gleam Street",
      "addressCountry": "AM"
    },
    "email": "william@times.ankh-morpork.xyz",
    "phone": "(555) 555-DISC (3429)"
  },
  "policyUrl": "https://times.ankh-morpork.xzy/privacy",
  "services": [
    {
      "serviceName": "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 end",
          "thirdPartyDisclosure": true,
          "thirdPartyName": "The Ankh-morpork Deadbeat Debt Collectors
Society"
        },
        {
          "purpose": "To personalize service experience",
          "purposeCategory": [
            "5 - Personalized Experience"
          ],
          "consentType": "Explicit",
          "piiCategory": [
            "1 - Biographical",
            "2 - Contact",
            "4 - Communications/Social",
            "7 - Financial"
          ],
          "primaryPurpose": false,
          "termination": "Subscription end date + 1 year end",
          "thirdPartyDisclosure": false
        },
        {
          "purpose": "To market services",
          "purposeCategory": [
            "6 - Marketing"
          ],
          "consentType": "Explicit",
          "piiCategory": [
            "1 - Biographical",
            "2 - Contact",
            "4 - Communications/Social",
            "7 - Financial"
          ],
          "primaryPurpose": false,
          "termination": "Subscription end date + 1 year end",
          "thirdPartyDisclosure": true,
          "thirdPartyName": "The Ankh-morpork Deadbeat Debt Collectors 
Society"
        },
        {
          "purpose": "Complying with our legal obligations",
          "purposeCategory": [
            "12 - Legally Required Data Retention",
            "13 - Required by Law Enforcement or Government"
          ],
          "consentType": "Explicit",
          "piiCategory": [
            "1 - Biographical",
            "2 - Contact",
            "4 - Communications/Social",
            "7 - Financial"
          ],
          "primaryPurpose": false,
          "termination": "Subscription end date + 1 year end",
          "thirdPartyDisclosure": false
        }
      ]
    }
  ],
  "sensitive": true,
  "spiCat": [
    "1 - Biographical",
    "2 - Contact",
    "4 - Communications/Social",
    "7 - Financial"
  ]
}
```

658 REVISION HISTORY

Version	Date	Summary of Substantive Changes
0.8 (Alpha)	2016-08-06	
0.9	2016-09-21	Significant restructuring of document and updates based on comments received.
0.9.1	2016-10-02	New Abstract and Introduction, editorial review and update of most sections, and updates based on WG feedback.
1.0.0 DRAFT 2	2016-10-19	• Further editorial updates. • Created tables for CR field definition, JSON field descriptions, and CR conformance.
0.9.3	2016-11-04	• More editorial work • Re-ordered and reconciled the field names and field order in the three tables and the schema.
1.0.0 DRAFT 1	2016-11-11	• Incorporated final comments from v0.9.3.
1.0.0 DRAFT 2	2016-12-16	• Final draft for WG approval

659