

# What is a Consent Receipt?

A consent receipt is a consent notice that is created at the point in which consent is provided. A receipt is intended to capture the policy and its protections so they can more easily be used. This way the consent can be used and referenced pre and post consent. In this way, a receipt is used to enable consent management, so that an individual can provide consent and later manage it. This way a decision to provide consent is not permanent. So that choices don't all have to be made at the same time.

A receipt can also enable an individual to manage consent outside of a company silo. This means consent management can be used to make one consent decision that can then be relayed to many companies at once.

For organisations that provide consent, it demonstrates; openness and willingness, to address privacy concerns and regulations. As a receipt is a tool that is used to encourage self regulation. Hence demonstrating a willingness and openness to be legally compliant with consent to regulators.

These benefits combined demonstrate the consent receipt as a tool of trust that is valuable for creating and maintaining loyalty with brands.

## Benefits

Individual benefit from Consent Receipts:

- Reduces friction around personal information sharing while adding transparency.

- Provides a record of personal data sharing transactions and associated permissions.
- Individuals can see, and better share, high value, high impact personal data in trustworthy ways with organisations.

For Business

The Consent Receipt:

- Reduces friction for their customer and the potential risk of engagement
- Improves the customer experience around personal information sharing,
- provides the platform for consent centric, high value flows of volunteered personal information between individuals and organisations

For Regulators

A consent record is proof of good personal information management practices within data controllers and processors.

Consent records can be used to expedite complaints, data access, and decisions for regulators. It reduces the burden on regulators and provides a framework for the customer and the organisation to self regulate.

A minimum viable consent receipt (MVCR), by itself, demonstrates an open communication channel between individual and organisations about policy.

-----

## Develop Consent Receipt's

Welcome to the development page for the consent receipt.

This section is currently being developed with this general outline:

1. Guide to Develop Consent
2. try the demo API – for consent receipt generator <http://api.consentreceipt.org>
3. use the api your self – create a consent receipt button
4. Generate a two party Consent Receipts – Guide to installing the API
5. Provide us with this feed back
6. Give direct input – CISWG

Currently we are using v0.7 of the consent receipt, and consent receipt generator, we call this version the MVCR (Minimum Viable Consent Receipt).

-----

## **Common Use Case: Consent Receipts for Explicit Consent On Websites**

Making consent receipts for websites.

The demonstration api, and the content for this website, are focused on the use case in which an explicit consent is provided online. This use case is used to illustrate the needed transparency over consent, and its benefits for information sharing.

The Guides provided here are for further illustration

1. Try the demo button to get a receipt
2. Try the demonstration api with our deme consent receipt form
3. Create your own consent receipt providing consent button with our demo api
4. Install the API yourself and provide consent receipts

-----

## Guides to Try

This is a guide to install this on your website:

1. Try the demo button to get a receipt
2. Try the demonstration api with our deme consent receipt form
3. Create your own consent receipt providing consent button with our demo api
4. Install the API yourself and provide consent receipts
- 5.

-----

# Feed Back

Give the consent receipt development community your feedback.. Fill in this form [form1]. Tell us if you are a user, a developer, or an interested organisation. Ask us a question, or give us your comments.

-----

## Consent Receipt: MVCR v.07 Specifcation Draft

This is the latest draft of the MVCR consent receipt specification. (note: the latest work can always be found in the Kantara Initiative github repository

<https://github.com/KantaraInitiative/mvcr>

KI-CISWG-Editorial-MVCR-V0\_7-20150907

Version.0.7.Read.me

In this version of the MVCR, there is also some experimental components. The first is the information sharing section, which is as yet, un-specified, along with a temporary set of PI attributes and purposes, which can be used to test the receipt, found in the appendix of the specification. Any implementation at this time should use their own purpose, but may find these references handy. Note: these are in no means definitive for the specification.

Current work effort status, we are developing some legal profiles, work-shopping purpose and attributes. we will also be having a receipt design session researching design requirements, with the ideas that purpose(s) can be represented by icons and the like.

Yet, the specification and its use to provide consent receipts make current adhesive consent practices more adhesive.

-----

## **Consent Blogs & Papers**

# **Benefits of Consent Receipt for Organisations**

by Iain Henderson

Managing consent, and the related permissions and preferences, is an ever growing challenge for organisations. Each new channel and

customer touch-point brings increasing complexity, and the ease with which data now moves around and replicates is a challenge to all parties involved.

Maintaining and refreshing consent adds further challenge, the customer or prospect does not wish to be bothered by regularly updating things that often mean very little to them, and yet has high expectations around accuracy, timeliness and relevance of messaging.

Third party sharing of consented data adds yet more fuel to the fire, whether from sharer or 'shared with' perspective.

And that's before we even think about the ever increasing regulatory burden emerging around consent.

Something needs to change to turn the above series of pain points into a more fruitful, easier to manage area going forward. That something is the Consent Receipt.

The simple act of providing a standard receipt to a data provider solidifies many aspects of the sourcing, management and use of personal data within organisations. Consider the different roles within organisations that are impacted by consent and permissions.

Consent Managers

The Individuals tasked with managing and using consent and related data most typically reside in the marketing function. They are at the sharp end, dealing each day with opt-ins, opt-outs, data quality, ability to contact customers and prospects, and the responses/engagement generated from that.

Improves customer experience. Provides solid refreshable record of consent that provides a solid platform for management and use of the related personal information.

Organisational processes that require access to personal information are being optimised as more data is shared, more frequently for jointly beneficial purposes.

Lawyers

Simplified responses to personal information queries, reduced costs.

Resources required to manage issues around personal data management and use are reduced

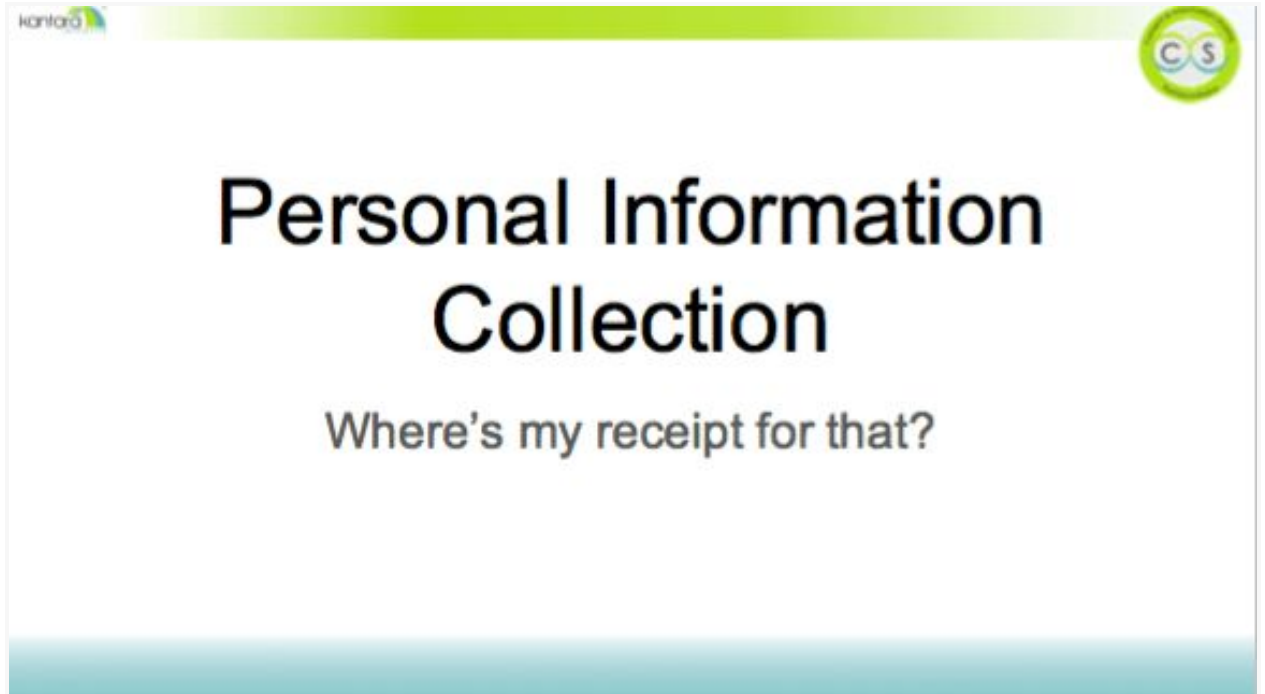
C-Level

Offers an opportunity for competitive advantage based on good practice in privacy and personal information use.

Toxic data sharing processes have been eliminated along with the risks associated; organisations are driving standards upwards.

Personal data management has become a key value add.





## **Consent Receipt Presentation at IIW-Oct-2016**

Presented Oct 26,2016 by John Wunderlich,

This Introduction to the MVCR (Minimum Viable Consent Receipt) explains how a consent receipt is an innovative consent notice and solves challenges that prevent people from sharing high value, personal information.

Posted on [27th November 2015](#) Categories [Presentations](#)

# Consent Receipts: Safe Harbour through Personal Data Control

(image and analytical background on Safe Harbor are in part inspired by an excellent business analysis & summary posted by Sotiris Spyrou & Posted in: Business, Cloud Data, SEO News.)

One of the biggest issues with moving data across jurisdictions is the different laws. This is in addition to the complexity of difference cultures and different contexts that create expectations of data use.

This is why data protection and privacy in the context of cross border data transfers is so difficult.

A preferred way to expedite data transfers is for people to control their own data and to consent to its access, rather than only its transfer.

A consent receipt is like a reverse (VRM) cookie, its a record that people get to track organisations and what they share about them. It collects the identity attributes that are provided, the purpose they are provided for and who they are shared with. The Consent Receipt can also carry assurances, trust marks, security promises and even reputations.

Combined with UMA, a consent receipt is a tool to show how personal control over data means that it can stay in a jurisdiction, and be shared with others. In essence people can control access to data and create their own Safe Harbor to transfer data across borders.

Regardless of who the data controller is, a key benefit of a consent receipt for organizations is the ability to add, record and provide

jurisdiction specific notice requirements to a consent notice.

Demonstrating compliance (or not) by the notices provided with the privacy policy for sharing and data use. Combined with model contract clauses, which are used to assure liability and define data controls, consent receipts address Privacy Policies while model contracts address Terms of Use.

In the EU, notice and consent is required for all personal data collection and sharing. In the US, explicit notices are required for consent for sensitive data. Data covered by federal laws like COPPA, GBLA, HIPPA, and the like.

In every jurisdiction sensitive data comes with specific, legally defined, notice requirements, that are localized. All sensitive personal data transfer requires explicit consent and notice that are intended to assure informed consent. It is for this reason that a consent receipt has been designed to highlight sensitive data, both what an individual considers sensitive and what the law considers sensitive, so that PII can be shared.

If an organisation doesn't meet legal notice requirements across jurisdictions, then it doesn't matter what model contract clauses are

used, the consent is not informed and compliant for sensitive data collection and sharing. In fact, model clauses can become a source of toxic liability and can be used to hold the data controller or processors liable. (which builds trust)

Posted on [23rd October 2015](#) Categories [Blog](#)

## Consent as a critical component for Trust in the Growth of the Digital Economy

July 27, 2015

Tags: [Kantara](#)

By Mark Lizar, CISWG Co-Chair, Kantara Initiative

In a day and age where sharing personal data is increasingly central to our social practices online and a requirement for the use of many services and applications, the capacity for users to understand and manage the data they share online is more important than ever.

Key to this is the notion of consent, which means that people explicitly agree to sharing, but at this time people can't independently track or control sharing using policies.



## Consent Is A Critical Component of Trust

By Mark Lizar, CISWG Co-Chair, Kantara Initiative

Re-posted from Internet Technical Advisory Committee

In a day and age where sharing personal data is increasingly central to our social practices online and a requirement for the use of many services and applications, the capacity for users to understand and manage the data they share online is more important than ever.

Key to this is the notion of consent, which means that people explicitly agree to sharing, but at this time people can't independently track or control sharing using policies.

In this regard, Kantara Initiative's Consent & Information Sharing Work Group (CISWG) is proud to announce our work on a Consent Receipt open standard. The Consent Receipt seeks to increase personal data control and transparency by increasing the capacity for people to track and manage data sharing relationships. We can build stronger trust in today's digitally driven economy by upgrading the digital consent and "I agree" buttons on and off the Internet so that

they provide users with a record of what personal information they have shared with a particular service.

The Consent Receipt serves people, organizations, and governments by addressing a lack of user trust. A Special Eurobarometer research report, released in June 2015, indicated a strong demand for consent, greater transparency, and more personal data control. This report is generated from a survey completed in March 2015. Approximately 28,000 respondents from different social and demographic groups were interviewed.

Sample quotes from the report reveal the current paradox: users are expected to provide consent with little or no information regarding what data they have consented to release.

“Nearly seven out of ten people (69%) say that their explicit approval should be required in all cases “.

“Yet only Only one fifth of respondents say they are always informed about the conditions of data collection and its potential uses when they are asked to provide personal information online.”

“Two-thirds of respondents (67%) say that they find privacy statements too long to read, while nearly four out of ten (38%) find them unclear or too difficult to understand.”

The Challenge – Usable and meaningful consent is obstructed by outdated practices and infrastructure. Policies and consent management today are having the effect of obscuring personal data control and eroding trust and innovation in the digital economy.

The Solution – A Consent Receipt is designed to solve this issue by increasing the capacity for people to manage personal information sharing. The development of a common way to record consent enables privacy policies to be layered, making them machine and human readable.



A standardized Consent Receipt effectively enables consent to be managed independently of service providers while affording the opportunity to make consent a positive customer experience.

Kantara Initiative is a participating Member of the OECD-ITAC. If you would like to learn more about the Consent Receipt work and how your organization can contribute or adopt please visit:

<http://bit.ly/ciswg>

Posted on [12th September 2015](#) Categories [Blog](#) [Leave a comment](#)

## **Benefits of Consent Receipt for Individuals**

Posted on [10th September 2015](#) Categories [Feature](#)

# Closed Consent

## Closed Consent

There is no common consent record format.

Information sharing is a complex issue for organizations that require consent for the collection of personal information. Legal obligations require privacy policies that reflect how personal information may be collected, used, disclosed, retained and disposed of or deleted.

Each organization has their own best practices, policy structures and policy formats. This results in a closed (or ‘siloe’) type of transparency, that violates the Openness (transparency and notice)

privacy principles, is very costly to manage for all stakeholders and very difficult to regulate effectively. This is compounded by each organization posting their policies in different locations, while frequently changing not only the content but also the URI of the policies.

The result is the current static and binary notice and consent infrastructure that is regulated, yet neither usable nor suitable for its intended purposes. An individual is asked to perform beyond what is reasonable in the current context.Â Each individual is expected to understand what information is being collected about them, how it will be used and for what purposes, with which types of entities their information will be shared and to understand and manage the consequences long past the first point of consent. All of this is without a record or the ability to manage consent independently out of context. Meanwhile, in context, people are expected to read all policies, keep track of all active consents, so as to be informed when making new consent agreements.

Information sharing is dramatically increasing, as a result, the capacity for people to manage information sharing also needs to increase. A specification for a core viable consent (or authorisation) will address specific jurisdictional requirements and provide a useful framework for developing compliance with ISO 29100 and other trust standards and frameworks.

Individuals' capacity to manage privacy is increased if they are able to aggregate and manage consent after it is provisioned. Digital consent records, which in this specification is called a consent receipt, enable people to manage information sharing relationships. Organizations can use these receipts to reduce friction and streamline the consent experience.

The core receipt specification addresses general, or regulatory, consent requirements. Consent receipts additionally become more useful as a channel for trust services, trust networks, identity federations, trust marks, privacy icons, standards, assurances, certifications and self asserted community and industry reputations.

## # Stakeholders

There are three general stakeholder audiences for the MVCR which are referenced through this specification:

### 1. People:

People receive the consent receipt and may use this to independently track consent and manage terms of sharing personal information.

### 2. Organizations:

Organizations provide consent receipts when they obtain or assume consent to collect personal information.

### 3. Regulators – (privacy and data protection enforcement)

Regulators include but aren't limited to the FTC in the USA, the Canadian Federal and Provincial Privacy Commissioners, the EU Data Protection Regulators. Regulators provide public processes for administration and enforcement of regulation in regards to notice and consent requirements

In summary, this MVCR receipt specification addresses the requirements of these three stakeholder groups with the aim to provide a self-regulatory market trust tool that organizations will implement, people can use, and regulators can enforce.

Posted on [26th July 2015](#) Categories [Blog](#) [Leave a comment](#)

## **European Identity Conference May 2015**

The Consent Receipt will make its debut at the largest EU Identity Conference.Â Mark Lizar will be presenting the Consent Receipt

and its use for making consent usable and identity profiles manageable.

The consent receipt represents the next generation digital freedom layer and is apart of making identity useable, trust worthy and meaningful.

Posted on [26th April 2015](#) Categories [Event](#)

## **Consent Meetup @ Mozilla London**

A great meetup with Hugo from TOS;DR inviting us to come together.Â Richard Beuamont, Reuben Binns, and StJohn from Citizen Me also made for an incredible meetup.

Thanks Mozilla and everyone for all the help.

Posted on [2nd October 2014](#) Categories [Event](#)

## Open Notice @ MIT Media Labs

Open Notice had theÂ opportunity of speaking at MIT Media Labs.

To join that likes of Sandy Pentland and John Klippenger on stage to discuss internet trust.



Posted on [18th September 2014](#) Categories [Event](#)

# Privacy Policy

Title: Open Notice Initiative Web Privacy Statement

Date: July 26, 2014

Revision: 1.0

Keywords: Privacy, “Open Notice”

# Open Notice Web Privacy Statement

## ## Summary

> This summary should be on the page or pop up where people click their consent

The Open Notice site will respect your privacy as much as possible. You should know that we do use cookies, but that other than technical data, no information that you give us about yourself will be shared with third parties. However, your browser may record that you have been at this site, and share that information on other sites.

## ## Collecting information from or about you

There are only two purposes for which we collect information about your or your browser when you visit our site; to operate a web service and to fulfill requests from you. It is the case that when you visit a web site, your browser exchanges information with our web servers. Some of that information is retained in web server logs. We collect, use, and retain as little of that as possible for as short a time

as is consistent with providing a reliable web service. Other than this, we will only collect information from you or about you when we tell you that we are doing so. For example, we might ask for your contact information for a mailing list, or to become a supporter of the Open Notice Initiative, or for a petition and so on.

**\*\*Cookies\*\*:** \*Our site uses cookies for statistical web traffic analysis.\*

## ## Using information from or about you

We use the information collected by the web server to maintain the web server and to troubleshoot any issues that may arise. That includes aggregate information about how people found our web site, what kind of browsers they are using, and other similar analytics. We use other information that you give us only for the purposes we identified at the time that we collected it.

## ## Disclosing information about you

We will only do this with your explicit permission. For example, if we run a petition campaign we might ask you if its OK to publish your name. We do analyze information about our web traffic using a third party service. We do our best to ensure that we provide the minimum information necessary to understand our web traffic, and that as much of the information as is possible is de-identified or aggregated, but you should know that this kind of service may be regarded as a disclosure of personal information in many jurisdictions.

You should also know that if we are asked for information from a legal authority we will ask for a warrant or equivalent instrument, but that if there is a legal authority for the information requested we will comply with the law.

## ## Retaining information about you

We will keep server logs for the minimum time that our service provider and technical best practices allow. Our target is 30 day retention but we cannot guarantee that. We will keep the information that you have provided us for as long as it is necessary for the

purpose you provided it. For example, if you have given us your contact information to keep in contact with you, we will keep that information and continue to use it until you tell us to stop. For specific campaigns, we will keep the information collected for the duration of the campaign, plus one year.

## ## Questions and complaints

If you have any concerns or complaints please send an email to [<privacy@opennotice.org>](mailto:privacy@opennotice.org).

-----

## About Consent Receipt's

- Consent Receipts are apart of the specification that is being developed in the Consent & Information Sharing Work Group at the Kantara Initiative
  - History of Consent Receipt Project
  - Get Involved
  - Provide Feedback
  - Consent Receipts – Legal Consent Notice
-

