The role of the Consent Management Solutions Best Current Practice WG

digi.me

kantara INITIATIVE

The Kantara Initiative's **Consent Management Solutions** Work Group

Has the goal of **developing** consent and privacy guidelines and standards…

As well as **integrating** existing guidelines and standards..

Through the **entire** customer lifecycle journey

Why ?

IoT

European Commission

Payment Services Directive,PSD2

CONSENT

U M A

SCOPE

Initial SCOPE of the WG

- To collect documented current practices for management of privacy notice and consent from many sources;
- To collect requirements from regulations in many jurisdictions;
- To publish a Kantara Recommendation "**Consent Management Solutions – Best Current Practices**" which is to contain consensus best current practices as derived from the sources;
- Once the initial scope is complete, additional publications will be scoped for production.

The publication describes the practices used by leading organizations to **manage the full lifecycle of an individual's consent to process their personal data**.
The lifecycle stages include privacy notice, prompt for acceptance of terms, collection of consent, production and storage of consent receipt, and, management of the record of consent.

The practices and requirements derived from them described in the publication can be used as the basis for a conformity assessment scheme which may include product and services certification.

AUDIENCE

The Audience of the WG:

- Organizations that collect personal information using individual consent for processing
- Identity providers and credential providers; Customer Information and Access Management (CIAM) providers
- Organizations in the ConsentTech, myData, “Internet of Me” spaces
- Privacy and Information Commissioners, Regulators
- Consent Management platform providers

WG leadership

Leadership team:

Chair: Corné van Rooij, iWelcome

Vice-Chair: Julian Ranger, digi.me

Secretary: Andrew Hughes, ITIM Consulting

Editor: TBD

Duration:

The WG will operate long enough to publish v1.0 and v1.1 of the Best Current Practices publication; no less than 12 months.

Consent in GDPR

- A data subject's **consent to processing** of their personal data must be freely given, specific, informed and unambiguous, **shown either by a statement or a clear affirmative action** which signifies agreement to the processing. **It can be withdrawn**.
- Consent must be "**explicit" for sensitive data**.
- The data controller is required to be able **to demonstrate that consent was given**. Existing consents still work, provided they meet the new conditions.
- Unless otherwise provided by member state law, controllers must obtain the **consent of a parent or guardian** when processing the personal data of a child under the age of 16.

- Full consumer Control over consent
- Auditability of consent, during the whole life of the consent
- Need to cater for parental consent

Consent in PSD2

- It is required that consumers give their **consent** to merchants **taking payments** from bank accounts directly via APIs
- The account holder has to give explicit **consent** if third party parties would like to **use data** for marketing purposes
- With consumer consent, TPPs (Third Party Payment service providers) have the opportunity to bring together key bank data, including income, purchasing history and debt repayments to obtain a 360 degree view of the consumer.

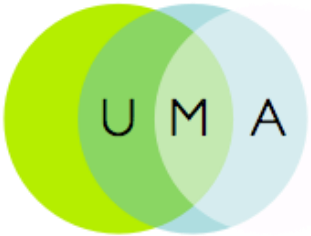
Consent (having it, using it !) is key.
Key for the banks, for PiSP's and for consumers.

Consent and UMA

UMA = User Managed Access

- UMA-enabled online services give individuals a unified control point for authorizing **who and what can get access to their online personal data** – such as email addresses, phone numbers, content such as photos, and services – no matter where those resources live online.
- UMA is built on top of OAuth V2.0 and OpenID Connect. These are the technologies that enable the **consent dialog boxes** seen on many websites and mobile applications.

UMA know two types: asynchronous consent & centralized consent management



Consent and IoT

GDRP impact on IoT:

- Requires users to receive a clear explanation of the privacy implications of a product and **give consent before any private data can be captured**.
- Requires IOT devices to be able to **obtain consent of sufficient quality** from users of such devices in relation to data processing activities.
- GDPR provides that consent **cannot be presumed** through the inaction of the data subject and that consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

- IoT devices face difficulty processing data if consent is not given.
- Consent likely needs to be managed outside the device itself.

Consent Lifecycle Management building blocks to think of…

Consent

- Request
- Change (Scope)
- Store (Record & Audit)
- Receipt
- View (Transparency & overview)

Consent Lifecycle Management Building Blocks

Consent to travel with the data….

HOW TO KEEP TRACK OF CONSENT ?

Consent Management Solution !

…extend the purpose, multi-value consent, give, pause, withdraw, etc.