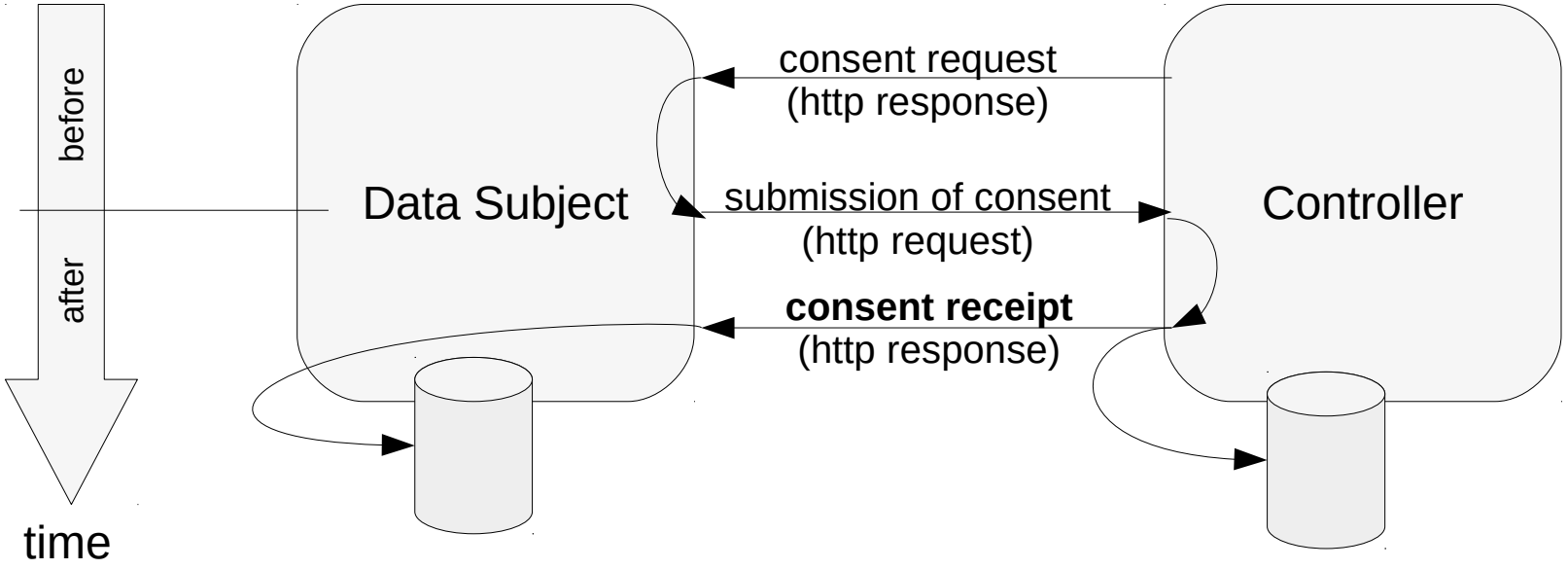
W3C DPVCG F2F Meeting
Vienna, 4/5 April, 2019

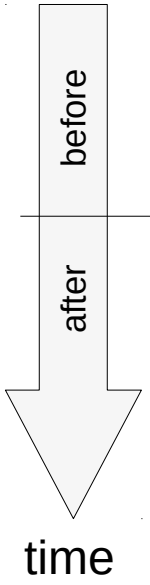
Consent Receipt and GDPR

Bud P. Bruegger

What is a Consent Receipt?



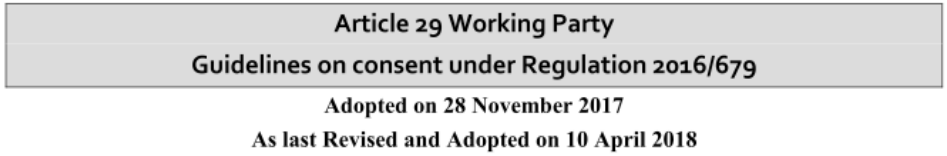
Users of a Consent Receipt and their interests



Data Subject	Controller
Elements necessary for a valid consent according to GDPR Metadata (date/time, a label)	
• how to exercise data subject rights (URLs) • authentication credential to access these rights	• data to “demonstrate consent” [Art. 7(1) GDPR]

Minimal Content to be "informed" according to GDPR

- Article 29 Data Protection Working Party: Guidelines on Consent:
  - controller's identity (who)
  - purpose of each of the processing operations (for which purposes)
  - what personal data (what data)
  - right to withdraw consent
  - use of the data for automated decision-making (where applicable)
  - possible risks of data transfers ++ (if transfer to 3rd country)


Article 29 Working Party

Guidelines on consent under Regulation 2016/679

Adopted on 28 November 2017

As last Revised and Adopted on 10 April 2018

Other possible content mentioned in GDPR

There are additional conditions for a consent to be valid

- Children
  - The „issuer" of the consent cannot be a child [Art. 8(1)]
    - „issuer" declares to be older than 16?
  - The „issuer" can be the holder of parental responsibility over the child
    - „issuer" declares to be holder of parental responsibility

- Data comes from Device (e.g., m-health) w/o user interface
  - Consent cannot be given on device itself
    - „issuer" declares/proves to be data subject of device data

Metadata on Submission

- Metadata is necessary to link the consent receipt to the related processing
  - Data Subject wants:
    - date & time of consent
    - a label for the service, for example:
      - URL of consent dialog
      - service name
      - self-chosen name
  - Controller wants:
    - date & time of consent
    - identifier that allows to link to the data subject

Subject Rights and Authentication

- Art. 7(3) GDPR: „It shall be as easy to withdraw as to give consent."
- Best approach:
  - Content receipt has URL where to withdraw consent
  - same for other data subject rights
- Authentication is necessary
  - e-mail is a bad approach
    - insecure (e.g., vulnerable to phishing), unencrypted
    - forces the controller to collect additional data
  - better:
    - identifier (pseudonym only used for data subject rights)
    - authentication code (e.g., HMAC of identifier)
      - needs to be stored securely (password manager)

Demonstrate Consent

- Art 7(1): „Where processing is based on consent, the **controller shall** be able to **demonstrate** that the data subject has consented to processing of his or her personal data.”
  - signature is ideal where possible
  - else: Art29WP:
    - ".. should not in itself lead to excessive amounts of additional data processing."
    - keep a record of consent statements received
      - == consent receipt

Demonstrate Consent Article 29 Working Party

- Art29WP: controller can demonstrate:
  - "when consent was obtained"
  - "information provided to the data subject at the time"
  - "that the data subject was informed" (how different?)
  - "controller´s workflow met all relevant criteria for a valid consent"

  - Example "online context"
    - "retain information on the session in which consent was expressed"
    - "documentation of the consent workflow at the time of the session"
    - "copy of the information that was presented to the data subject at that time"

Demonstrate Consent Article: 29 Working Party *(gray: author's interpretation)*

- Example "online context"
  - "retain information on the session in which consent was expressed"
    - raw HTTP request (including "Remote_Addr") of consent form submission
  - "documentation of the consent workflow at the time of the session"
    - constant for long periods
    - include a digest of the consent dialog page (plus linked content) in consent receipt?
  - "copy of the information that was presented to the data subject at that time"
    - unless the consent dialog spans multiple pages, workflow and content are both contained in the web page.
- All could be encrypted with a public key to restrict the use of this data to demonstrate consent.