Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

GEANT Data Protection Code of Conduct 2.0

BARBARA MONTICINI

Roma, 9 maggio 2018

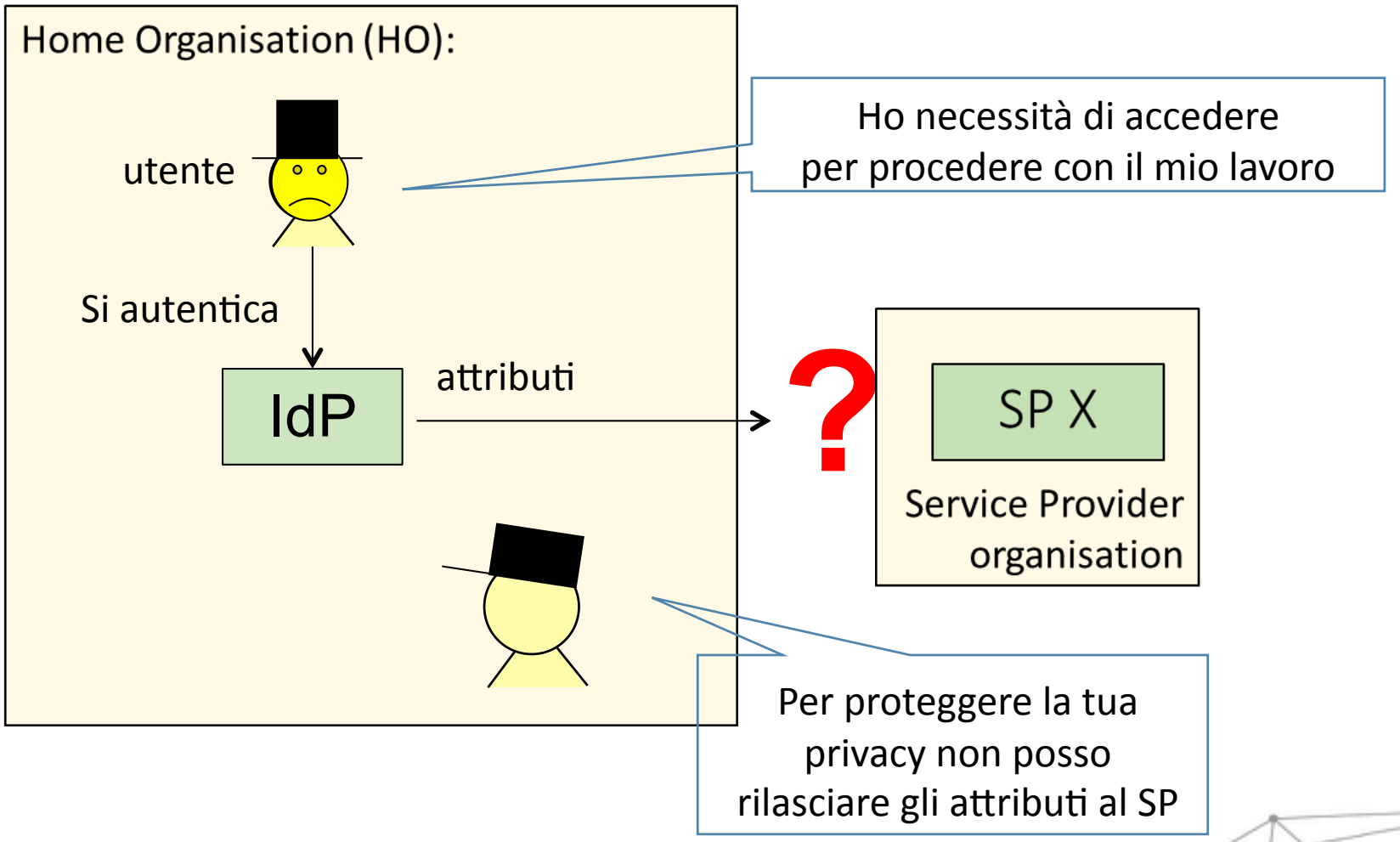
IDEM day 2018

Argomenti

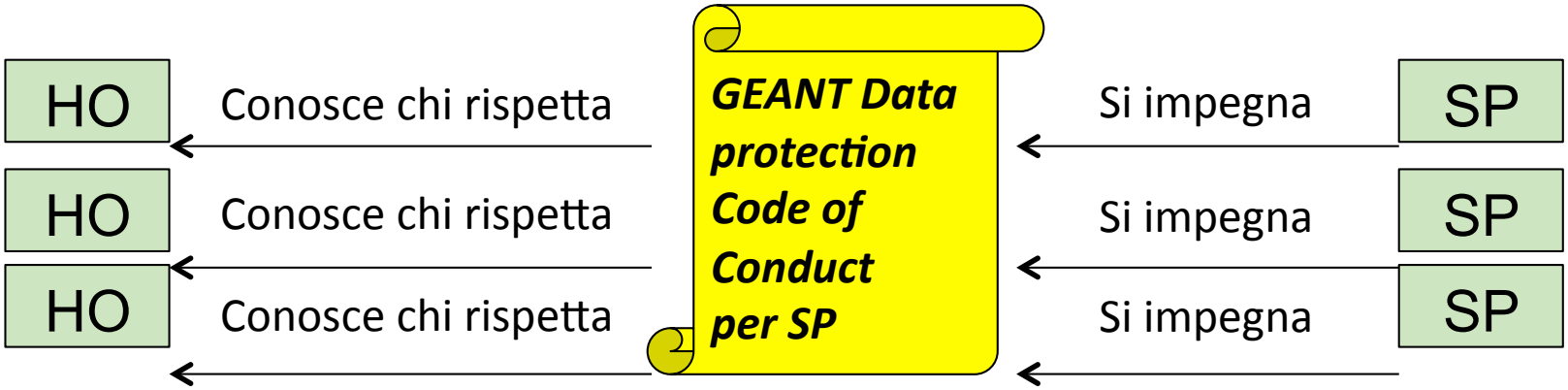
- Il problema del rilascio degli attributi
- L'approccio del Codice di Condotta per SP
- … un po' di storia
- La versione 2.0 del Codice di Condotta
  - I vantaggi di avere CoCo «GDPR approved»
  - La nuova struttura
  - Gli obblighi del SP
  - SP non-conformi & CoCo monitoring body
  - Prossimi passi
- CoCo in IDEM

Draft della nuova versione https://wiki.refeds.org/x/QADSAQ

Il problema del rilascio attributi



L'approccio di CoCo



- Service Provider (SP) si impegnano a rispettare CoCo
- Le Federazioni (eduGAIN) trasmettono tale informazione alle Home Organization:
  - ✓ attraverso i metadati SAML2 (Entity Category)
- HO può decidere se aderire a CoCo e fidarsi dell'impegno preso dai SP che hanno aderito a CoCo

GEANT CoCo … un po' di storia

GEANT CoCo version 1.0 (attuale)

- Lavoro iniziato nel 2011, sviluppato tramite pilot nel 2012-2013
- Pubblicata nel 6/2013
- Sottoposto data protection authorities (WP29)
- WP29 (2015): CoCo 1.0 non ha valore aggiunto
  - CoCo dovrebbe specificare il significato dell'applicazione della direttiva nel contesto delle federazioni d'identità
- 4/2016: viene approvato il GDPR
  - L'uso di codici di condotta è incoraggiato

⇒ CoCo 2.0 ambisce a definire regole rivolte ai principi del GDPR

- Prima consultazione pubblica nel 2-4/2017

I vantaggi di avere CoCo «GDPR approved»

Anche se non strettamente necessario avere CoCo approvato da una supervisory authority

... se un codice di condotta viene approvato certi aspetti acquisiranno un valore più vicino ai requisiti della legge:

- **Accountability**
  - Aderire ad un Codice di Condotta approvato "*may be used as an element by which to demonstrate compliance with the obligations of the controller and the processor*." (art. 24 & art. 28 GDPR)
- **DPIA**
  - La conformità con un Codice di Condotta approvato "*shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment* " (art. 35)
- **Data transfers to 3rd countries**
  - Aderire ad un Codice di Condotta approvato "*together with binding and enforceable commitments by organisations outside of Europe may be the legal basis for data transfers without requiring any specific authorisation from a DPA*" (art.46)

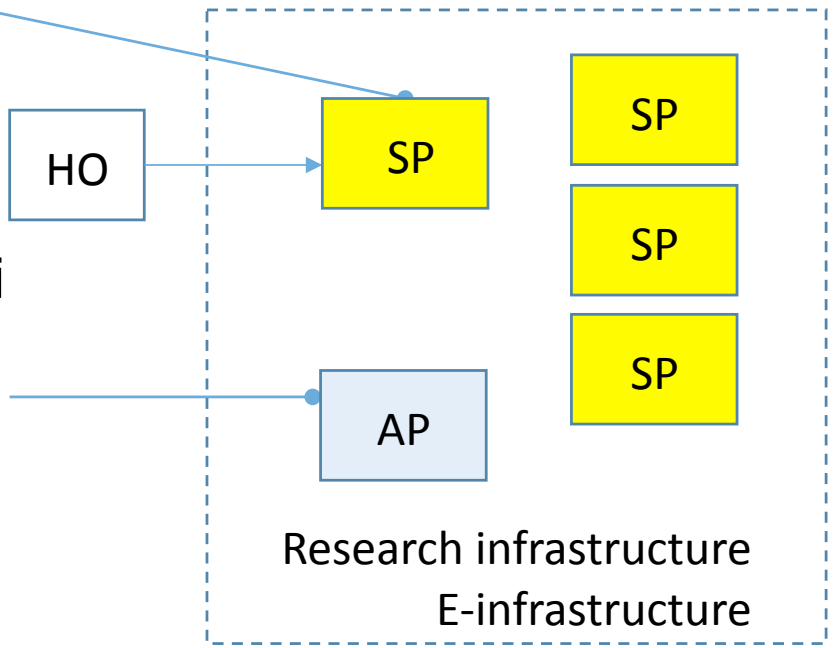
Ambito territoriale

- SP di EU e EEA (EU28 + Norway, Iceland, Liechenstein)
- SP di nazioni della EC whitelist e organizzazioni internazionali (”*forniscono livelli adeguati di protezione*”)
- SP di altre nazioni e organizzazioni internazionali (Art. 46.2(e): ”*together with binding and enforceable commitments*”)

Service Provider Home Organisation	In EU/EEA or EC whitelist	Outside EU/EEA or EC whitelist
In EU/EEA or EC whitelist	Yes	Yes (with binding and enforceable commitments)
Outside EU/EEA or EC whitelist	Yes	(Yes)

Ambito applicativo

- L'applicazione di CoCo è limitata all'insieme degli attributi che la Home Organization rilascia **per garantire l'accesso ad un Servizio**
- I SP (comunità) possono includere in tale insieme anche gli attributi ottenuti da altre fonti
  - Es. Attribute Provider (AP) provenienti da una community



- Fuori dal contesto:
  - Contenuti da fonti esterne
  - Dati personali che il SP raccoglie direttamente dall'utente

La nuova struttura

Principles of the Processing of attributes

a) Legal compliance
b) Purpose limitation
c) Deviating purposes
d) Data minimization
e) Information duty towards End User
f) Information duty towards Home Organisation
g) Data retention
h) Security measures
i) Security breaches
j) Transfer of personal data to third parties
k) Transfer of personal data to third countries
l) End User's consent
m) Liability
n) Governing law and jurisdiction
o) Eligibility
p) Termination of the Code of Conduct
q) Survival of the Code of Conduct
r) Precedence

Appendices

- Appendix 1: Information duty towards End Users
  - I. How to develop a Privacy Notice
  - II. How the Home Organisation should inform the End User on the Attribute release
- Appendix 2: Information Security, technical and organisational guidelines for Service Providers
- Appendix 3: Handling non-compliance of service providers
- Appendix 4: Glossary of Terms

Obblighi per i Service Provider in CoCo

Scopo del trattamento: attivare l'accesso al servizio
- Per altri scopi: consenso

Data **minimisation**: attributi adeguati, rilevanti e non eccessivi

Data **retention**: cancellare i dati non più necessari

Inform duty: Informativa per l'utente -> privacy notice template

Security measures: Sirtfi

Security breaches: informare le Home Organization

Release to 3rd party: se si tratta di un data processor, se aderisce a CoCo, se c'è consenso utente

Release to 3rd countries: se CoCo o con appropriate tutele

Liability: SP solleva dalle colpe la Home Organization

Precedence: contratti bilaterali, CoCo, GDPR

Jurisdiction: regolato dalle leggi Olandesi (a meno di accordi tra le parti)

SP non-conformi & CoCo monitoring body

- Gli operatori di Federazione possono nominare un "*monitoring body*". Se nominato dovrà essere accredito presso una *supervisory authority*
  - ogni *monitoring body* segue gli SP relativi alla propria federazione
- Independente
- Può richiedere alla Federazione la rimozione del tag CoCo dai metadati dei SP che commettono violazioni
- le decisioni possono essere impugnate facendo appello ad una *supervisory authority* competente

Prossimi passi

Percorso legale

25 May 2018 sarà sottoposto ad una supervisor authority

- European Data Protection Board darà un parere su CoCo
- EC pubblicherà CoCo in caso positivo

Percorso tecnico

Aggiornare il documento con la nuova versione

Aggiornare ”CoCo SAML 2.0 metadata profile” ”CoCo Entity Category specification”

Aggiornare il tool CoCo monitor: monitor.edugain.org/coco

CoCo in IDEM

Ad oggi hanno aderito a GEANT CoCo:

- 37 Identity Provider
- 19 Service Provider

Per conoscere lo stato delle entità di IDEM:

https://monitor.edugain.org/coco