THE ITALIAN RESEARCH & EDUCATION NETWORK | Consortium GARR

Il Codice di Condotta per i Service Provider in eduGAIN, la Privacy, il rilascio degli attributi con le Entity Category

Maria Laura Mantovani <marialaura.mantovani@garr.it>

GARR WS17 | Roma, 6.4.17

Che cos'è? Si mangia?

- Directive 95/46/EC
- D. Lgs 196/2003
- Regulation 2016/679 (GDPR)

Disclaimer: I'm not a Lawyer, but…

- Legal advisor:
  - Patrick Van Eecke
  - Enrique Gallego Capdevila

- Commitment:

NB: Questa presentazione ha solo carattere informativo e non costituisce in alcun modo un parere legale

Agenda

1. Introduzione a Data Protection Regulation
2. Il trattamento dei dati personali nell'architettura delle federazioni di identità secondo principi di liceità:
    - Codice di Condotta per SP
    - Scopo del trattamento
    - Base legale
    - Dati personali trattati: Attributi
    - Consenso
    - Conservazione
    - Informativa
    - (Identificativi)
    - (Pseudonimizzazione)
    - Entity Category

introduzione

La legge favorisce la circolazione di dati personali?

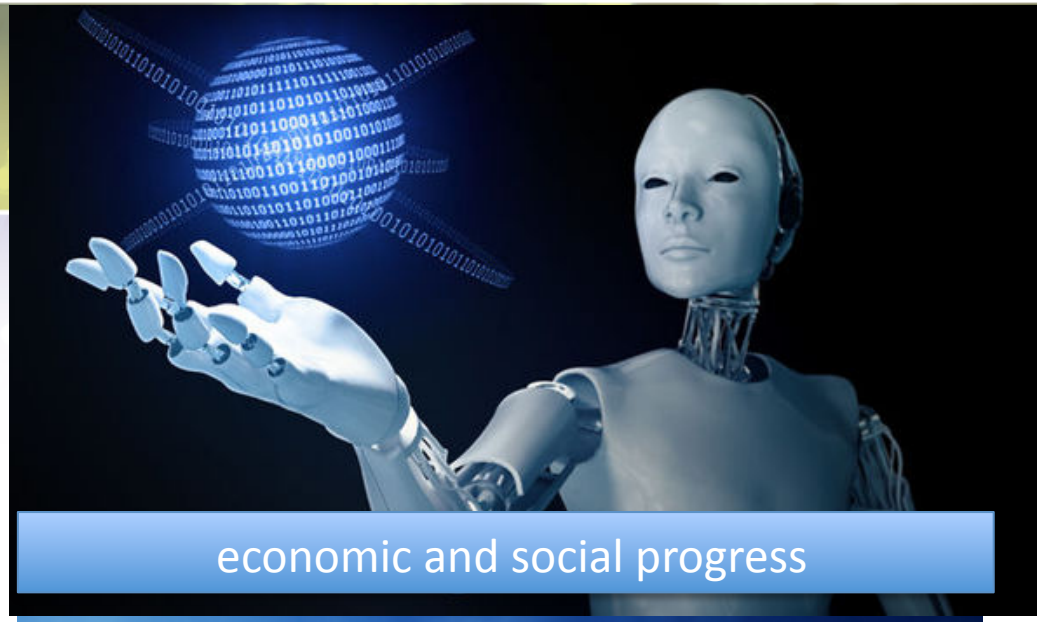
Articolo 1 Oggetto e finalità

1.Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

2.Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

3.La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

accomplishment of an economic union

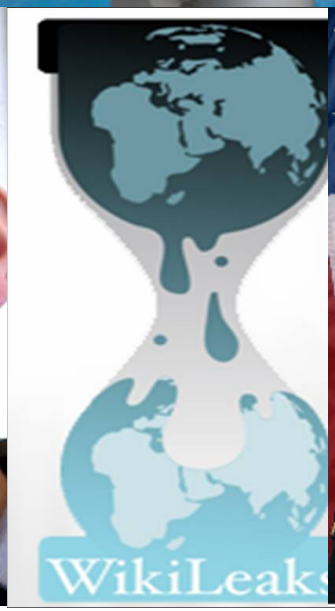


economic and social progress

strengthening and convergence of the economies within the internal market,

well-being of natural persons

Patrimonio – Diritti della persona



Data Protection Regulation

- Directive 95/46/EC: on
  individuals with regard
  personal data and on t
  data
- D. Lgs 196/2003: CODI
  PROTEZIONE DEI DATI
- GDPR: REGULATION on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

GDPR: del 27 aprile 2016

La direttiva 95/46/CE è abrogata a decorrere dal 25 maggio 2018.

Libera circolazione dei dati vs. Rispetto dei diritti delle persone

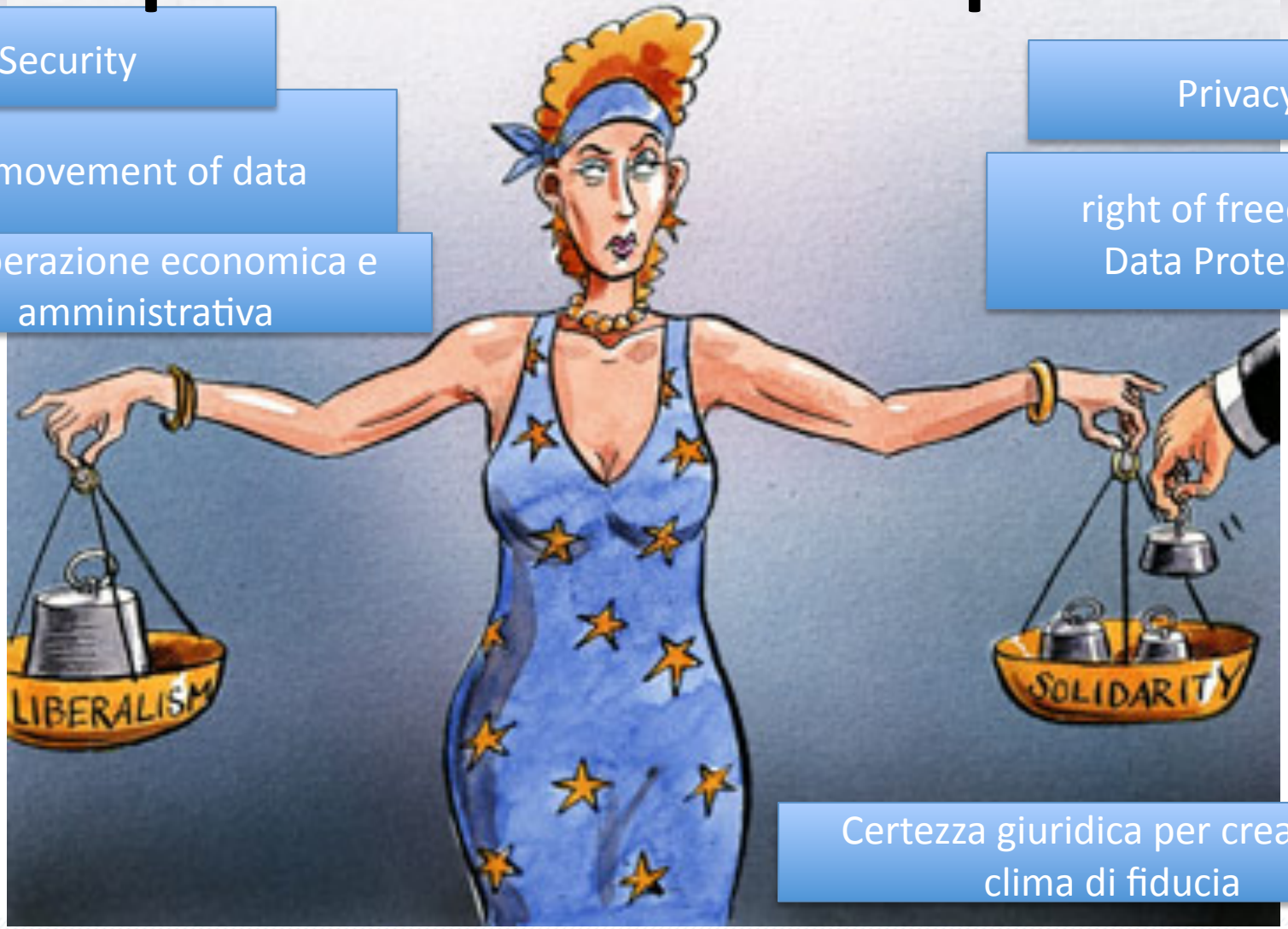
Security

free movement of data

Cooperazione economica e amministrativa

Privacy

right of freedom = Data Protection



Certezza giuridica per creare un clima di fiducia

Libera circolazione dei dati vs. Rispetto dei diritti delle persone

(5)L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali e quindi anche dei dati personali scambiati, in tutta l'Unione, tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese. Il diritto dell'Unione impone alle autorità nazionali degli Stati membri di cooperare e scambiarsi dati personali per essere in grado di svolgere le rispettive funzioni o eseguire compiti per conto di un'autorità di un altro Stato membro.

(6) La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

(7) Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche.

Come si tutelano i diritti?

- Certezza del diritto in uno spazio geografico ampio
- Trattamento lecito
- Trattamento corretto
- Trattamento trasparente
  - Informazione all'interessato su trattamento e esercizio dei diritti
  - Interessato ha diritto di accesso, rettifica e cancellazione di dati, diritto alla portabilità dei dati, diritto di opporsi, di essere informato dell'esistenza di una profilazione e delle conseguenze della stessa, diritto di ricevere comunicazione su violazione di dati personali
- Protezione dei dati
  - La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate

Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro.

Protection by design e Protection by defult. Misure di sicurezza quali ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile.

il problema del rilascio degli attributi (Personal Data) nel sistema delle federazioni di identità

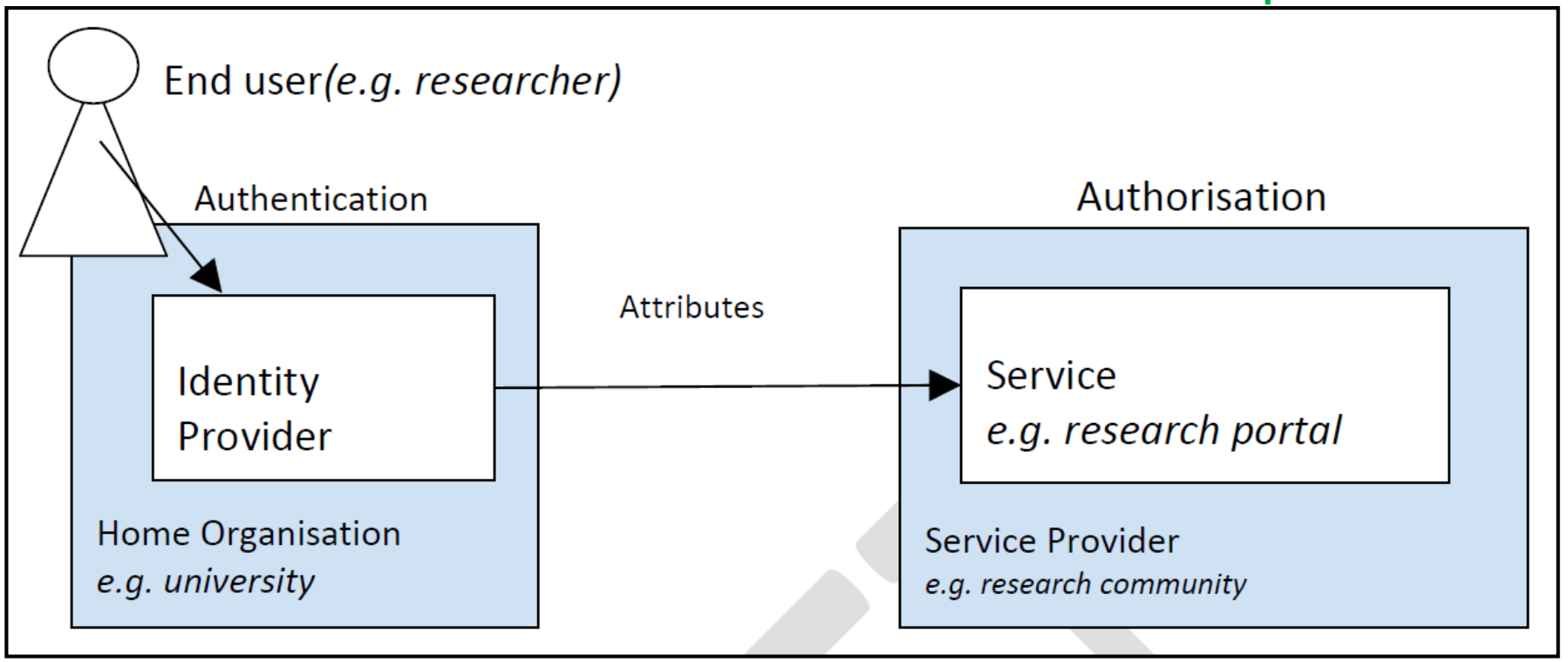
Contesto: eduGAIN la AAI dell'e-infrastructure GÉANT

La Federazione IDEM, come le altre Federazioni Nazionali di Identità, appartengono alla interfederazione eduGAIN.

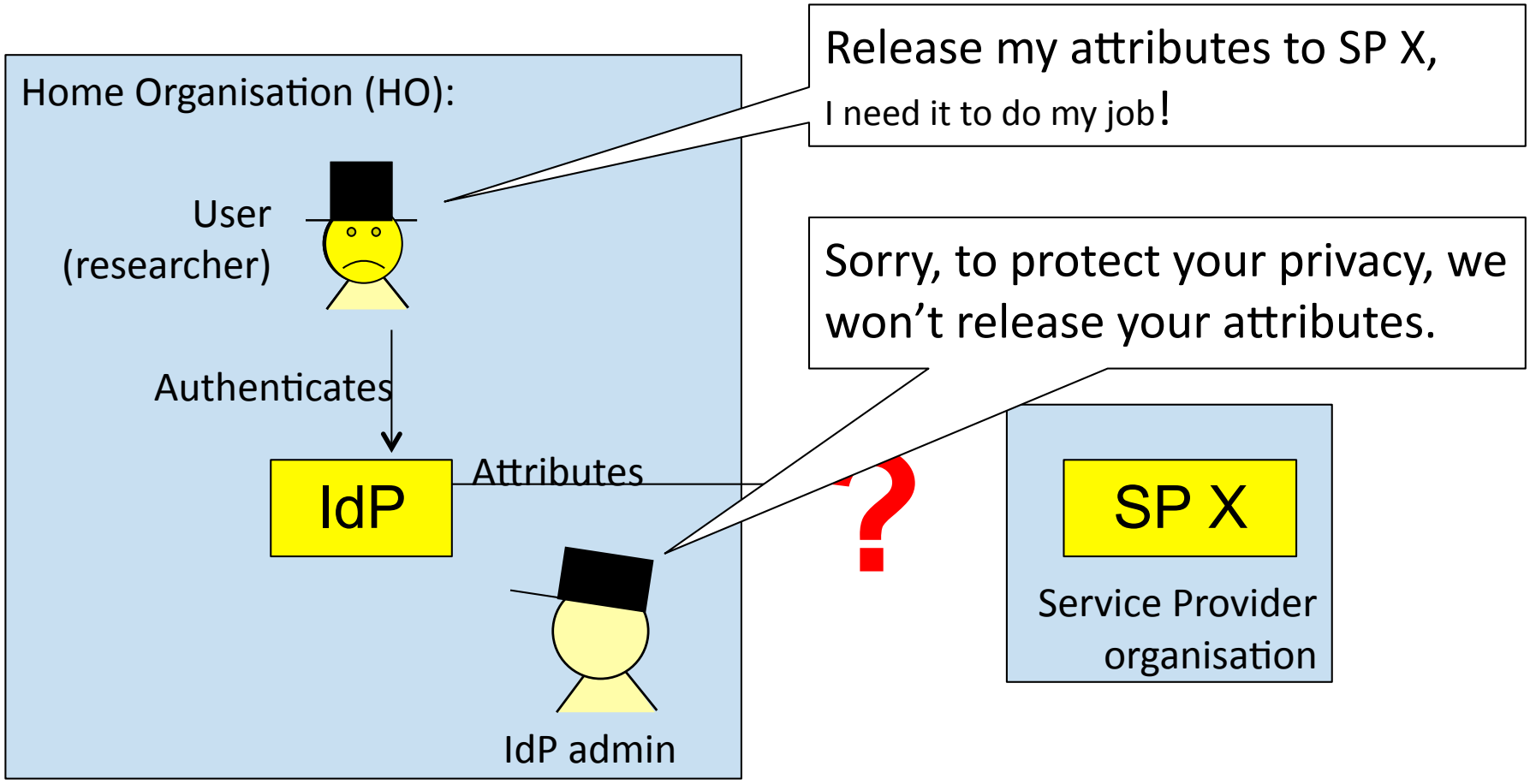
- Milioni di End User
- Oltre 2300 IdP
- Circa 1500 SP
- Oltre 40 paesi

eduGAIN risponde ai principi del GDPR:

- **Sicurezza e fiducia**
- **Data protection by design e by default**
- **Minimizzazione dati personali**



The data protection challenge in federated identity



Attributes are personal data. The data protection laws must be followed.
To be on the safe side, many Home Organisations hesitate to release attributes.

Soluzione: GÉANT Data Protection Code of Conduct

Data protection Code of Conduct (CoCo) version 1.0 for SPs in EU/EEA or the EC whitelist

- Version 1.0 (6/2013)
- 106 Service Providers
- 112 Home Organisations

CoCo submitted to European data protection authority (WP29) in 12/2014

- Answer received in 06/2015:
  - The CoCo is not wrong, but something is missing
  - The CoCo must explain what the law means in the context of R&E federations

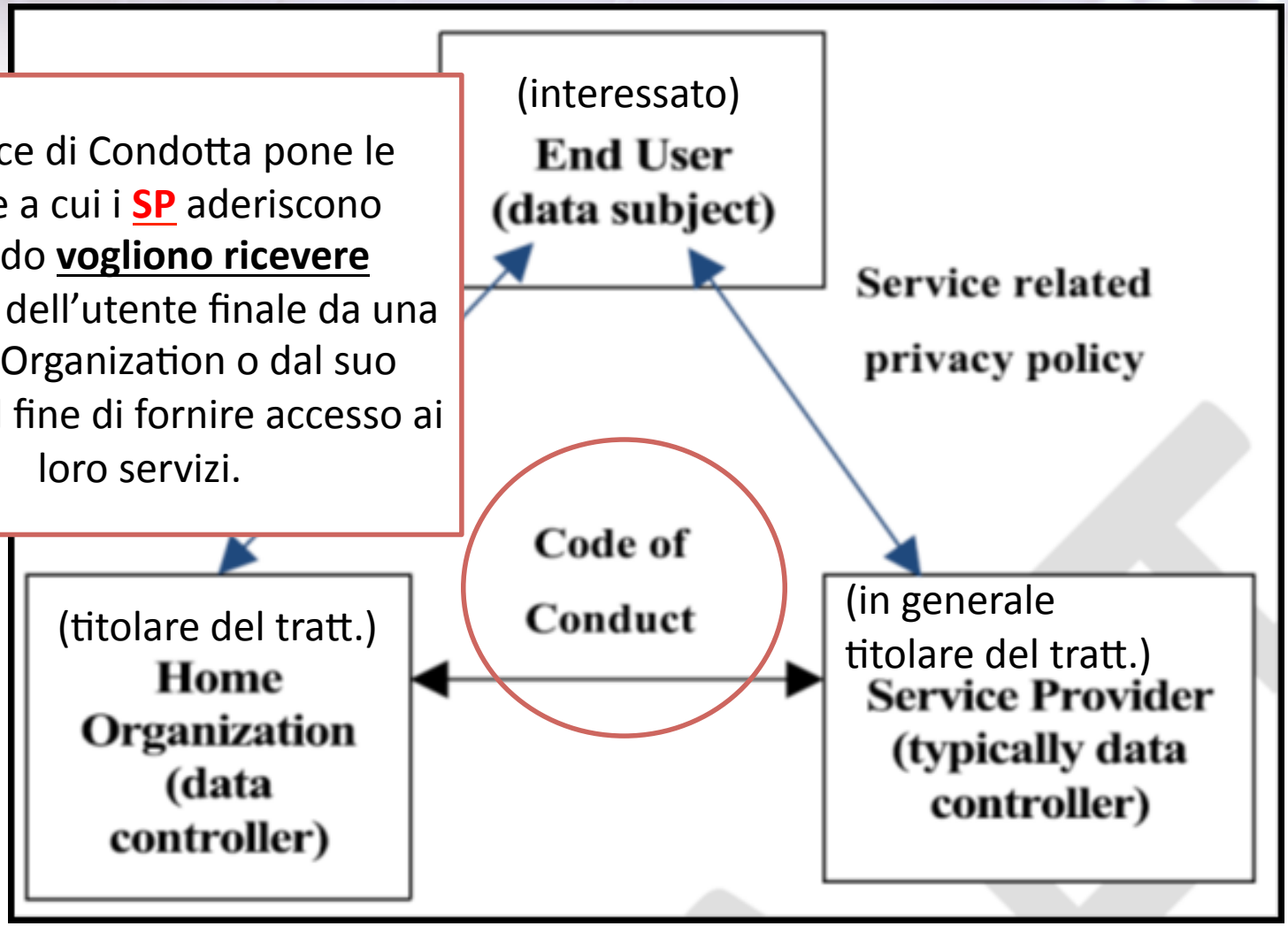
Code of Conduct 2.0 DRAFT (02/2017)

1. Addresses the WP29 comments
2. Addresses the General Data Protection Regulation
3. Addresses attribute release out of EU/EEA
   - GDPR introduces approved CoCo as a means for the release to a 3rd country
   - International organisations

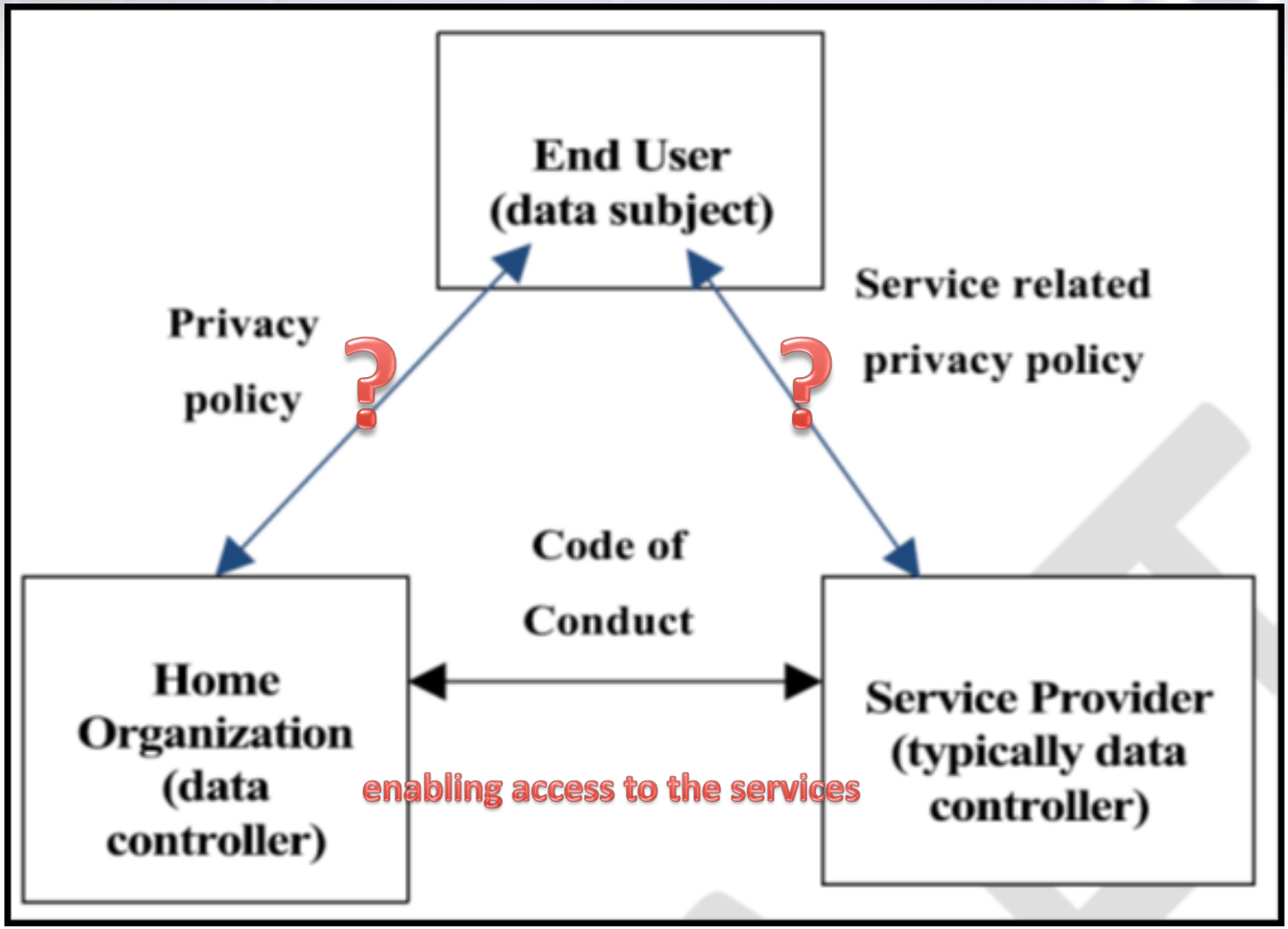
Open for comments until 22 Apr2017, then resubmitted to WP29

Ruolo delle parti in relazione al GDPR

Il Codice di Condotta pone le regole a cui i **SP** aderiscono quando **vogliono ricevere Attributi** dell'utente finale da una Home Organization o dal suo Agente al fine di fornire accesso ai loro servizi.



Scopi del trattamento
Purposes of processing



Purpose limitation: «enabling access to the services»

- **Authorisation**: gestire il diritto dell'utente di accedere ai servizi del SP sulla base degli Attributi
- **Identification**: l'utente ha bisogno di essere identificato per avere accesso ai propri files, datasets, pages, documents, postings, settings, etc. …
- **Transferring real-world's trust to the online world**: i membri di una community che si conoscono nella vita reale, vogliono potersi riconoscere anche on line, mediante la visualizzazione del loro nome
- **Researcher unambiguity**: assicurare che il contributo scientifico di un riceratore sia associato correttamente a lui e non alla persona sbagliata
- **Other functionalities offered by the Service Provider for enabling access**: ad esempio per inviare notifiche dal servizio all'utente, o per invitarlo ad accedere al servizio richiesto

Attributi: quali posso chiedere?

- la HO dell'utente, e l'unità organizzativa, il suo ruolo e posizione nella HO (se sono membri dell'università, studenti o staff amministrativo, ecc…) e, per esempio, i corsi che stanno seguendo o insegnando (esempi: eduPersonAffiliation, eduPersonEntitlement or schacHomeOrganisation)
- un identifier (identificativo) (come SAML2 PersistentId, eduPersonPrincipalName oppure eduPersonUniqueID)
- il nome (come cn o DisplayName)
- un identificativo di disambiguazione (ad es. ORCID o ISNI)
- contatti a scopo di notifica (email, mobile, …)

Principio di minimizzazione

identificativi

Base legale: legittimo interesse dei titolari

Il trattamento effettuato da SP allo **scopo** di «abilitare l'accesso ai servizi» ha come **base legale** il **legittimo interesse del titolare** (GDPR art.6 c.1(f)).

Questo è l'unico scopo coperto da CoCo 2.0.

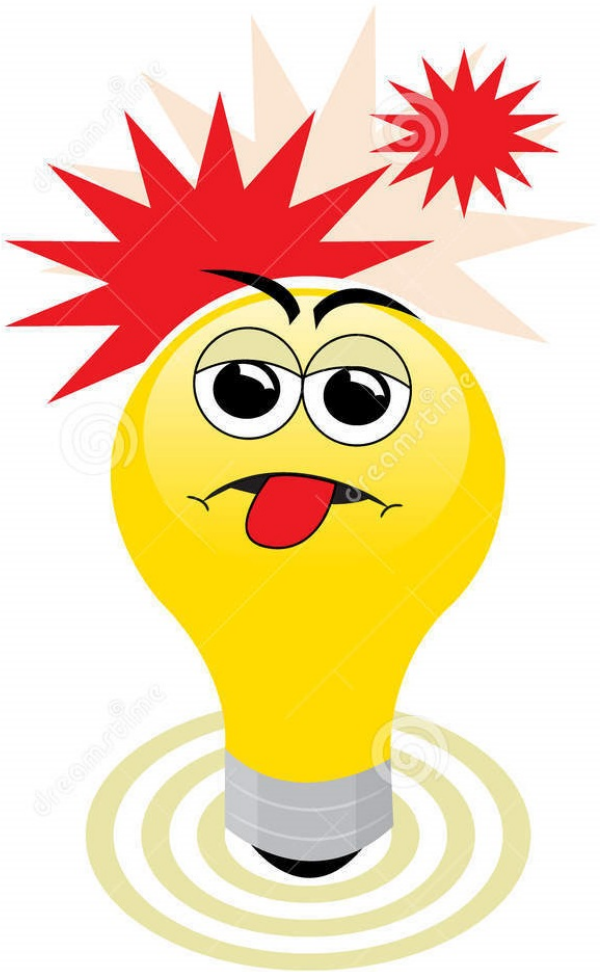
Se il SP vuole usare gli attributi ricevuti dell'IdP per altri scopi, deve chiedere il consenso all'utente

(Esempi di altri scopi sono:

- includere l'indirizzo email dell'utente nei destinatari di una news letter che offre nuovi servizi,
- vendere gli Attributi a terza parti,
- trasferire le informazioni a terze parti come la history della ricerca,
- attività di profilazione, ecc.)

Base legale:
Devo chiedere il Consenso?

- informato,
- specifico,
- dato liberamente,
- non ambiguo,
- revocabile (anche on line)



Se gli **scopi** del trattamento sono quelli descritti dal codice di Condotta (abilitare all'accesso), il consenso non si deve chiedere. Si usa invece come base legale il legittimo interesse del titolare.

Per quanto tempo posso tenere gli attributi?

- cancellare o anonimizzare tutti gli Attributi appena non sono più necessari per gli scopi di fornire il servizio.
- periodo di conservazione deve essere deciso dal SP
- NO periodo di tempo illimitato o indefinito
- documentare nella privacy policy
- buona pratica cancellare o anonimizzare i dati personali dell'utente finale se non si è più collegato da 18 mesi

Motivi validi per data retention:

- Se il servizio è un repository, un git, un archivio dove i ricercatori pubblicano le loro scoperte scientifiche e i loro contributi, i loro dataset, i ricercatori vogliono mantenere il loro nome e altri attributi collegati ai loro dati anche se non si collegano regolarmente.
- Se il servizio è una applicazione collaborativa (come un wiki o uno strumento per la discussione) dove l'utente finale ha il suo nome e altri attributi collegati ai propri contributi per far sapere agli altri utenti la provenienza del contributo ed attribuirlo ad una persona specifica.

Per quanto tempo posso tenere i log?

I dati personali, inclusi i file di log, non necessitano di essere cancellati o anonimizzati finché sono necessari:

- Per scopi di archiviazione nel pubblico interesse, scopi di ricerca storica o scientifica o scopi statistici
- Per conformità con un obbligo legale che richiede il trattamento in forza della legge dell'unione o dello stato membro a cui il SP è soggetto
- Per effettuare un lavoro nel pubblico interesse
- per costituire, esercitare o difendere un diritto per via giudiziaria, come ad esempio l'allocazione delle risorse o delle fatture;
- per esercitare il diritto di libertà di espressione o di informazione

Devo dire per cosa uso i dati?

La Privacy Policy deve essere concisa, trasparente, intellegibile, e fornita in forma facilmente accessibile,

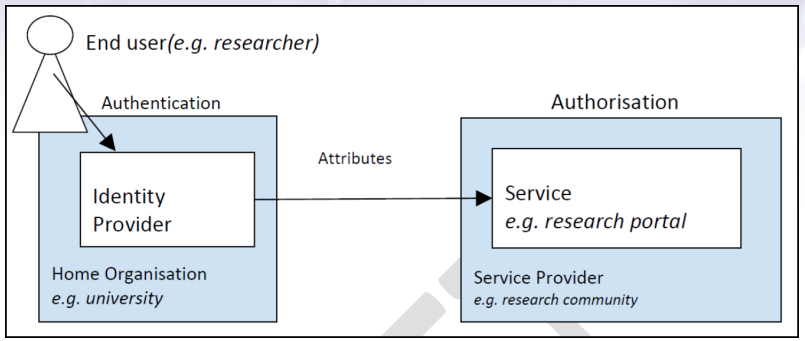
La Privacy Policy deve contenere almeno le seguenti informazioni:

- Il nome, l'indirizzo, la giurisdizione del SP
- I dettagli di contatto del titolare del trattamento, dove applicabile
- Gli **scopi** del trattamento degli attributi
- Una **descrizione** di come gli attributi vengono trattati e la base legale per il trattamento
- Le terze parti riceventi o le categorie di terze parti riceventi a cui gli attributi potrebbero essere trasmessi e la possibilità di trasferimento degli attributi a paesi fuori dll'EEA;
- L'esistenza del diritto di accesso, rettifica e cancellazione degli attributi mantenuti riguardo l'utente
- Il periodo di conservazione
- Il riferimento a questo codice di condotta
- il diritto di presentare una denuncia presso l'autorità di vigilanza

Entity Category

<http://www.geant.net/uri/dataprotection-code-of-conduct/v1>

IDP può trasferire legalmente gli Attributi a SP se in anticipo conosce se il SP aderisce a CoCo.
Non serve accordo bilaterale tra IDP e SP.



SP fornisce nei metadati:

a) Un link alla privacy policy

b) Indicazione di adesione a questo codice di condotta

Inoltre:

c) Comunica se cambia la legislazione nel suo paese

GÉANT ha predisposto una soluzione tecnica scalabile che permette ai SP di dichiarare la loro aderenza a questo codice di condotta e comunicare la propria privacy policy URL. Questa informazione viene condivisa con gli IDP server delle HO prima che esse trasferiscano gli attributi dell'utente ai service provider.

IDP rilascia gli Attributi ad un SP, solo se SP appartiene all'insieme di coloro che aderiscono al CoCo.

La soluzione tecnica consente di recepire dinamicamente la modifica dell'insieme dei SP.

L'utente viene informato del possibile rilascio degli attributi prima che questi vengano inviati ed ha la possibilità di consultare la Privacy Policy nel momento della richiesta di uso di un servizio

MET

Metadata Explorer Tool

Search service ID

Login

Entities summary | Most federated entities | Interfederations summary | Federations summary

I cookie ci aiutano a fornire i nostri servizi. Utilizzando tali servizi, accetti l'utilizzo dei cookie da parte nostra.
Maggiori informazioni qui. Chiudi.

Consortium GARR

Accedi a Metadata Explorer Tool

Username

Password

Non ricordare la login

Ripulisci i permessi di rilascio di informazioni dati a questo servizio in precedenza.

Login

› Dimenticata la password?

› Serve aiuto?

› Pagina di informazioni

› Privacy Policy

Il Metadata Explorer Tool permette rapidamente di trovare le federazioni, le entità e le relazioni tra di esse nei metadati che le descrivono.

› Informazioni aggiuntive sul SP

I cookie ci aiutano a fornire i nostri servizi. Utilizzando tali servizi, accetti l'utilizzo dei cookie da parte nostra.
Maggiori informazioni qui. Chiudi.

Descrizione del SP

Il Metadata Explorer Tool permette rapi
le entità e le relazioni tra di esse nei me

‹ Torna alla pagina di login

› **Descrizione:**
Il Metadata Explorer Tool permette rapi
le entità e le relazioni tra di esse nei me
› **Organizzazione:**
Metadata Explorer Tool erogato da Géa
› **Organizzazione:**
Metadata Explorer Tool erogato da Géa
› **Contatti:**
Marco Malavolti
› **Privacy Page**
› **Sito di informazioni**

Il Progetto IDP in the Cloud (GARR), partecipa ad **IDEM** (**IDE**ntity **M**anagement federato per l'accesso ai servizi) per la realizzazione dell'Infrastruttura di Autenticazione e Autorizzazione federata della rete GARR.
Il rilascia credenziali d'accesso per questo sistema di autenticazione (Identity Provider) ai propri dipendenti e ai ricercatori affiliati.

GÉANT Association (NL) | https://met.refeds.org/static/pr

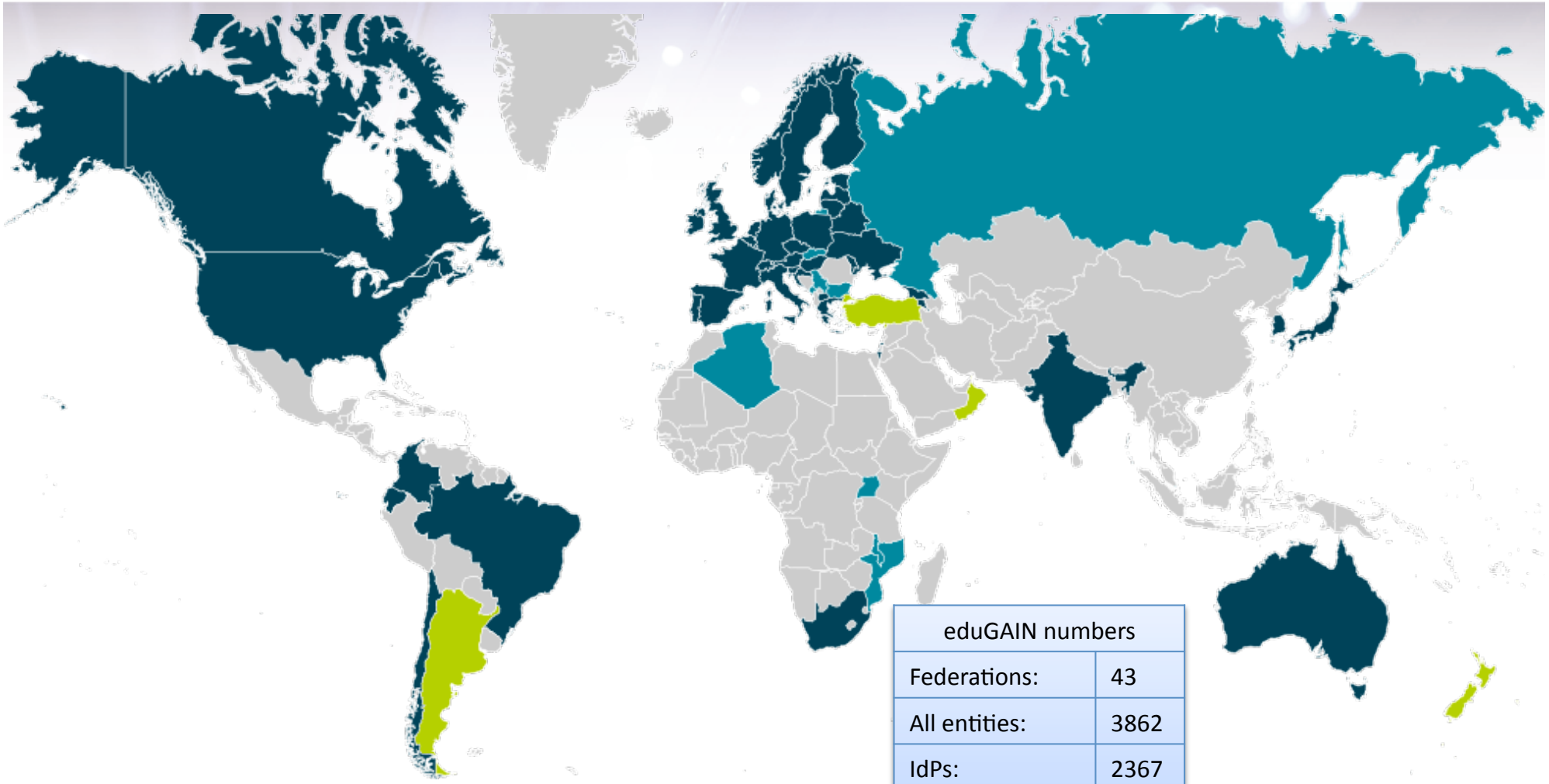
Nome del servizio	Metadata Explorer Tool
Descrizione del servizio	Il Metatadata Explorer Tool permette rapidamente di trovare le federazione, le entità e le relazioni tra di esse nei file che le descrivono.
Titolare del Trattamento e contatto	Consortium GARR, info @ garr.it
Dati personali trattati	Per gli utenti autenticati I seguenti dati vengono trasmessi dall'organizzazione di appartenenza dell'utente: • ePPN (O) per ottenere l'accesso al sistema, • mail (O) per ricevere notifiche dal sistema, • givenName (R) per assegnare il nome appropriato all'utente loggato nel sistema, • surname (R) per assegnare il cognome appropriato all'utente loggato nel sistema
Finalità del trattamento dei dati personali	I dati personali degli utenti autenticati vengono usati per determinare il permesso di lettura e di scrittura di ciascuna pagina. Per coloro che hanno il permesso di scrittura, i dati personali sono usati per identificare l'utente (conoscere chi ha fatto modifiche e a quali pagine).
Destinatari a cui possono essere comunicati i dati	I dati di log non saranno rilasciati a terzi, eccezion fatta per ottemperare agli obblighi di legge. Gli utenti autenticati che editano pagine devono essere consapevoli che potenzialmente il loro identificativo utente può essere visibile ad altri utenti del wiki.
Come verificare, rettificare e cancellare i propri dati personali	Contattare idem-help @ garr.it. Per rettificare i dati rilasciati dalla propria organizzazione di appartenenza, contattare l'help desk IT della propria organizzazione.
Durata del trattamento	I dati personali sono cancellati su richiesta dell'utente o se questi non ha utilizzato il servizio per 2 anni.
Codice di Condotta per la Protezione dei Dati Personali	I suoi dati personali saranno protetti in accordo con il Codice di Condotta per i Service Provider, uno standard comune per il settore della ricerca e dell'istruzione per proteggere la sua privacy.

This privacy policy is based on the Data protection Code of Conduct Privacy policy guidelines for Service Providers

Chi potrà aderire al CoCo 2.0?

- qualsiasi SP stabilito in uno qualsiasi dei 28 stati membri della EU e in ogni altro paese appartenente alla EEA (28 membri + Islanda, Liechtenstein, Norvegia)
- i SP stabiliti in un qualsiasi paese terzo che offre un adeguato livello di protezione dei dati nei termini dell'art 45 del GDPR
- Il GDPR dà l'opportunità ai SP che non ricadono nell'ambito territoriale del regolamento e sono stabiliti fuori dalla EEA di aderire a questo codice di condotta per fornire le appropriate garanzie nel quadro dei trasferimenti di dati personali verso i paesi terzi o le organizzazioni internazionali sotto i termini riferiti nel punto (e) dell'art. 46(2) del GDPR.

Geografia eduGAIN



eduGAIN Voting-only Candidate

eduGAIN numbers	
Federations:	43
All entities:	3862
IdPs:	2367
SPs:	1499
Standalone AAs:	4

Domande?

Thank you for your attention!

Domande

- Quali SP devono applicare le norme EU? Se stanno fuori EU?
- Devo dimostrare che sto facendo quanto è necessario?
- Chi mi controlla?
- Ci sono dati più sensibili di altri?
- Posso collezionare tutti i dati che voglio?
- Devo preoccuparmi della sicurezza dei dati?
- Cosa devo fare se i dati vengono violati (data breaches)?
- L'interessato può chiedere che i suoi dati vengano corretti?
- L'interessato può chiedere di ricevere indietro i propri dati?
- Posso dare in outsource le mie attività di trattamento di dati personali?
- Posso memorizzare i dati ovunque?

Bibliografia

- https://wiki.refeds.org/download/attachments/1606455/GEANTDataProtectionCodeOfConductV2_23022017.pdf
- https://wiki.refeds.org/display/CODE/GEANT+Data+Protection+Code+of+Conduct+workshop+22+Feb+2017
- https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home
- https://wiki.edugain.org/Data_Protection_Code_of_Conduct_Cookbook
- https://wiki.geant.org/display/AARC/Legal+Outreach+and+Dissemination
- GDPR http://eur-lex.europa.eu/eli/reg/2016/679/oj
- https://www.dlapiper.com/~/media/Files/Other/2016/DLA_Piper_GDPR_Comparison.pdf
- http://www.garanteprivacy.it
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6059229
- https://wiki.geant.org/display/aaastudy/AAA+Study+Workshop
- G. Ziccardi. Internet, controllo e Libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica. Raffaello Cortina Editore