



Science and
Technology
Facilities Council

GDPR news

WLCG GDB meeting, 14 October 2020

David Kelsey, STFC, UK Research and Innovation

WLCG Privacy Notice

- Approved in 2019
- <http://wlcg-docs.web.cern.ch/wlcg-docs/?dir=policy/security>
- Should be presented to users of all WLCG services
 - Service needs to prepare its own if general WLCG PN does not work
 - Including all LHC experiment services too
- What is the current status of deployment?
 - Are services hosted at CERN still waiting for approval of their RoPO?
 - RoPO = Record of Processing Operations
- Are there examples of RoPO for CERN IT scientific services?

Personal Data Policy Framework

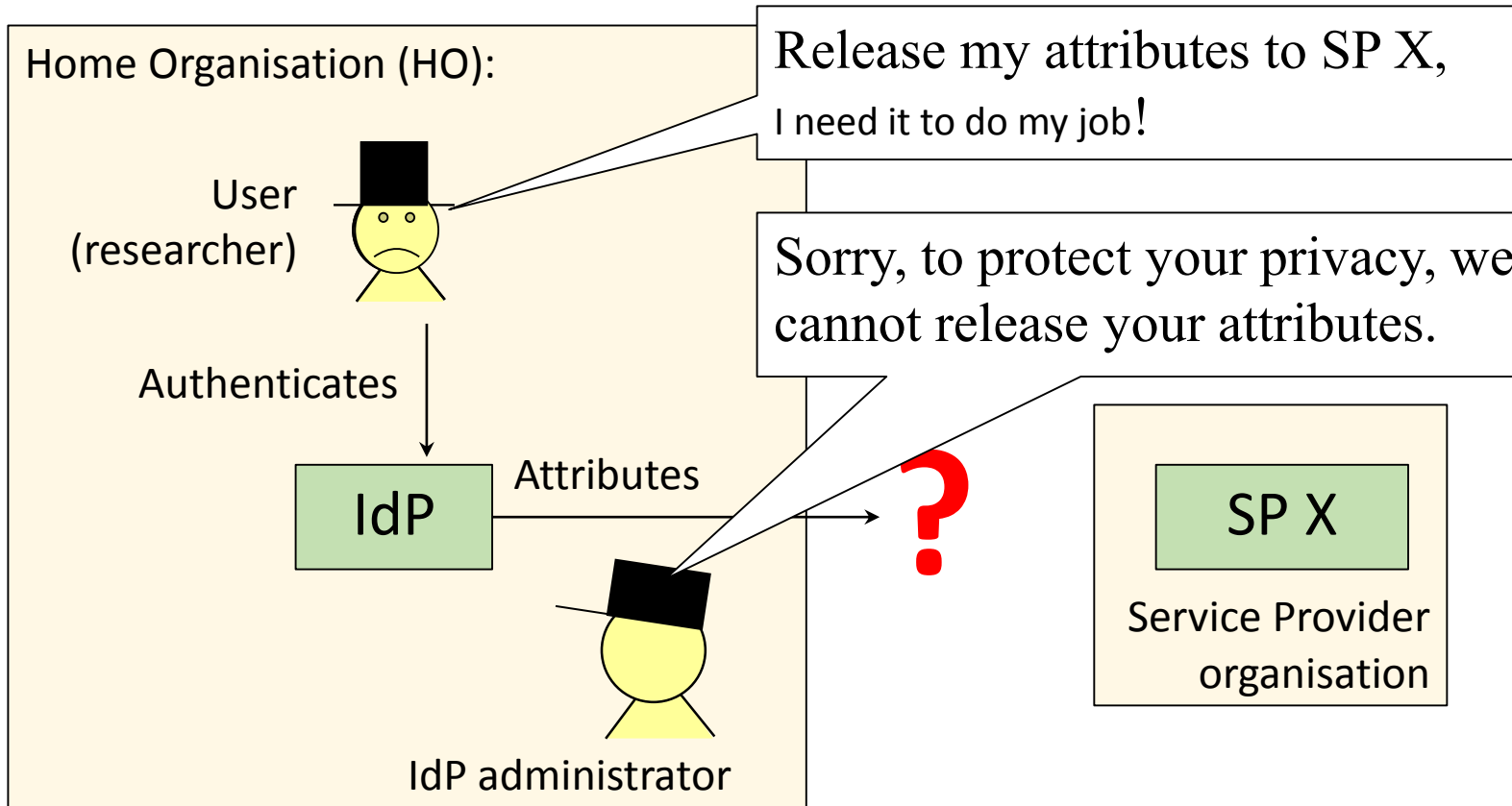
- The old framework (2017) still applies
 - <https://wlcg.web.cern.ch/computer-security>
- Updated draft “Processing of Personal Data Policy Framework” was discussed
 - https://docs.google.com/document/d/1X6m8FhLHH3qe5pIWOZQYoYJKt_z6oHJo6euDB1Y3e6s/edit
- Lots of discussion during 2019
 - But draft was never finalised
 - We concentrated on the WLCG Privacy Notice
 - Waiting also for CERN to make progress on “Records of Processing Operations” for Scientific IT services
- We were also waiting/hoping for the new **GEANT DP Code of Conduct version 2**
 - Status of this changed in recent months – see next slides

GEANT Data protection Code of Conduct

Infoshare 8 June 2020

Mikael Linden, mikael.linden@csc.fi
GEANT project, CSC – IT Center for Science

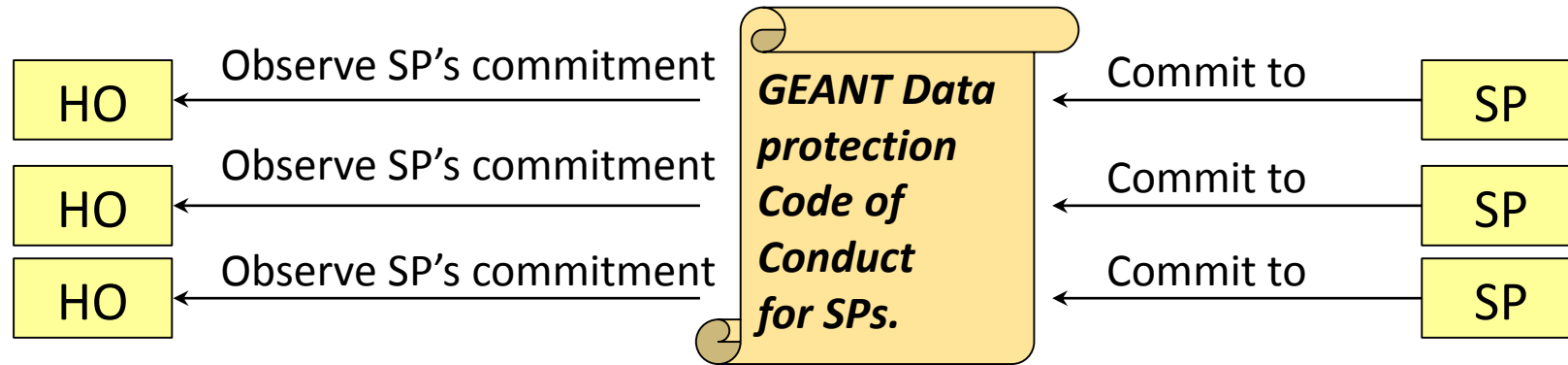
The attribute release challenge: Why a Code of Conduct is needed



Typical user attributes [personal data]:

- name
- e-mail address
- unique user identifier
- role and affiliation (“student@universityx.org”)
- dedicated permissions to use the service

GEANT Data Protection Code of Conduct (CoCo) approach



- Service Providers (SP) commits to the CoCo
- Identity federations (and eduGAIN) relays SPs' commitment to Home Organisations (HO)
- HO decides if it feels confident to release attributes to the SP

Code of Conduct ver 1.0

- Code of Conduct, SAML2 entity category and SAML metadata profile
- Published 6/2013, has a status of “good practice”
- 205 SPs (in 21 federations) committed, 430 IdPs (20) respecting

Code of Conduct ver 2.0 draft

- work started in 2016 when GDPR published
- aiming at a formal approval by authorities
- EDPB guidelines for codes of conduct 6/2019
 - “EDPB will publish separate guidelines for codes for international transfers”
- informal meeting with Dutch (GEANT’s home) authorities 20 Jan 2020

<https://wiki.refeds.org/display/CODE/Code+of+Conduct+ver+2.0+project>

An approved CoCo gives some extra powers

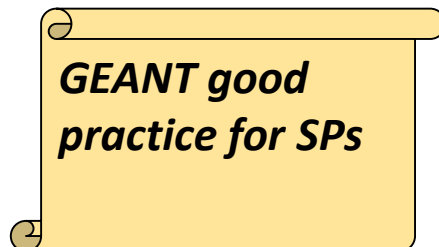
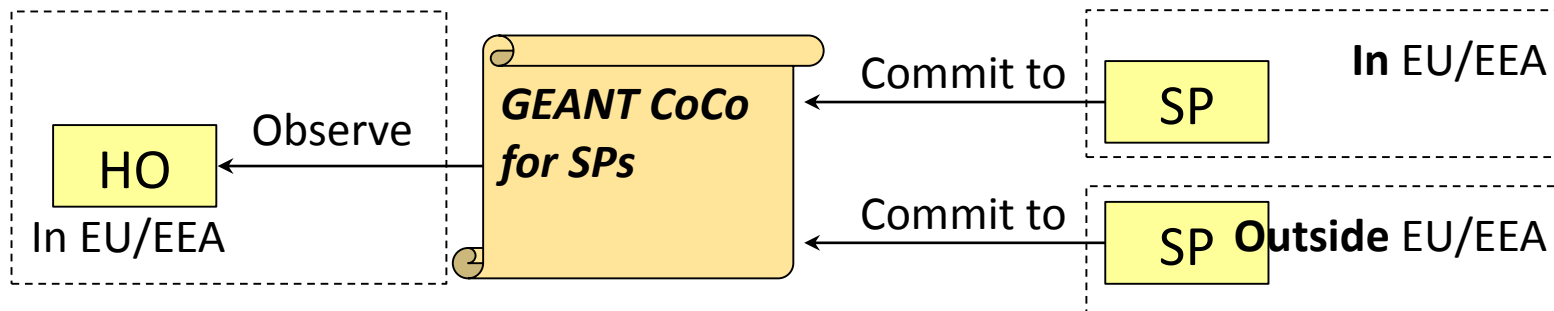
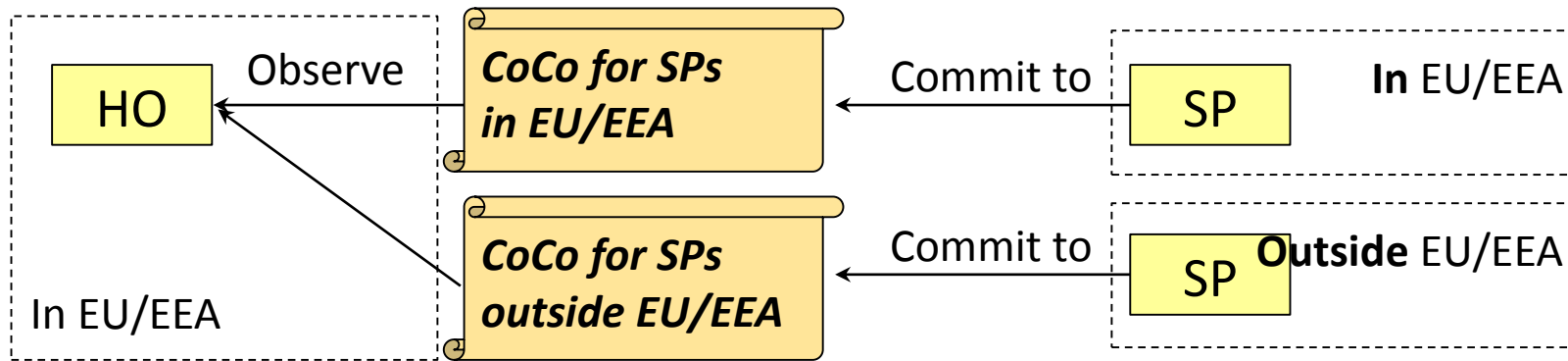
- contributes to demonstrating proper information security (Art 24, 28, 32)
- contributes to the Data Protection Impact Assessment (Art 35)
- can enable international transfer (Art 46)

GÉANT and DLAPiper (our law firm) has arranged a meeting with the Dutch DPA

- The Dutch DPA has shown interest in assisting our community in preparing the GÉANT CoCo for the EDPB approval
- However... The Dutch DPA came back with some Q (next slide)

1. Currently not possible to approve a CoCo for international transfers (including International Organisations, e.g. CERN, EMBL, ESA)
 - due to the pending EDPB guidelines
2. The monitoring body has no power to monitor public authorities' SPs
 - GEANT must collaborate with DPA for them
3. Dutch DPA assuming submitting its criteria for monitoring bodies in April
 - enables us to formally submit GEANT CoCo
 - currently assuming GEANT Association as the monitoring body

Our options for next steps (decision needed!)



Option 1: proceed in two steps

- Reduce current CoCo's scope to SPs in EU/EEA
- Develop CoCo for SPs outside EU/EEA later when guidelines available

Option 2: wait until guidelines

- put the work on hold until EDPB guidelines on CoCos for 3rd country release available

Option 3: Stop developing CoCo

- publish the current CoCo as a GEANT good practice (c.f. CoCo 1.0)
- no authority blessing

End of Mikael's slides from June 2020

Decision on approach to Geant CoCo V2

- Option 1 was the most popular, so my understanding is that that will be followed
- When will EDPB guidelines on International Codes of Conduct be published?

Next steps for GEANT project

- Modify the Code of Conduct V2 to be EU/EEA-only
- Submit to Dutch DPA (when?) – approval when?

Next Steps for WLCG

- Delayed (International) Code of Conduct V2 means
 - We should continue work on the updated WLCG DP Policy Framework
- Aiming for a good draft for wider discussion
 - Address all issues raised last year
 - Security Policy teams have been busy on other tasks
 - And EU H2020 project obligations
- Aim to complete the good draft before end of 2020
- Note that the existing policy is not bad!

But the **more urgent** activity:

- **Continue deployment of WLCG Privacy Notices**



Science and
Technology
Facilities Council

Questions?

Facebook: Science and
Technology Facilities Council

Twitter: @STFC_matters

YouTube: Science and
Technology Facilities Council