DP CoCo 2.0 Workshop

TIIME, 22nd February 2017

Links

- A draft of the Code of Conduct is now available on-line and open for comment until April 22nd 2017
- https://wiki.refeds.org/download/attachments/1606455/GEANTDataProtectionCodeOfConductv2_21022017.pdf

- The coordinates for the workshop:
- https://wiki.refeds.org/display/CODE/GEANT+Data+Protection+Code+of+Conduct+workshop+22+Feb+2017

Motivation for joining workshop

- Fed Ops dealing with data protection issues for IdP operators
- SPs hoping to get more attributes by asserting CoCo
- Infrastructures want to understand how to act legally
- EMBL/CERN/ESA looking to understand how intergovernmental organisations can deal with GDPR and whether the CoCo helps us
- Supporting research collaboration across borders
- Fed Ops trying to understand whether GDPR will hurt or help
- Non-EU SPs trying to ensure they meet European guidelines

Background

- 5 years worth of work, using DLA Piper as legal input
- 106 SPs committed to code of conduct
- 112 IdPs willing to release attributes to them
- WP29 asked to review, conclusion was that CoCo must add value and explain GDPR in R&E FIM context
- Now v2.0 draft addresses WP29 comments & GDPR

Main changes v 1 -> 2

- Explain what data protection means for service providers
  - Attributes only used for enabling access to the services
  - Real world to online trust conversion (e.g. real names used if appropriate)
  - Researcher unambiguity (scientific contribution is correctly recorded)

Roadmap

- Comments until April 22nd
- Integrate comments
- Iterate with data protection authorities (WP29)
- Submit to EC on May 25th 2018
- Downside of iteration with DP bodies is that CoCo seems to grow, making it less approachable for technologists
- Will have informal contacts to WP29 before the submission and expect to know whether the CoCo can be approved by WP29
- Apparently this CoCo is the first to be submitted to WP29

Do I really process personal data?

- Attributes = Personal Data
- Still same definition, anything identifiable -> harmonised definition to avoid countries going down different paths

Do I need to apply EU rules?

- Yes
- GDPR applicable worldwide -**> any 3rd country processing EU citizen's data will need to comply with the GDPR for the data "producer" to legally transfer it**
- For FIM community, any non-EU federation (+participants) needs to comply with GDPR
- Data protection authorities & european court of justice police organisations. Sanctions could include
  - Blocking web services (doesn't try to tackle people accessing non-compliant services via e.g. Tor)
  - Forcing services to change practices, e.g. Google & right to be forgotten
- Aiming for data protection authorities in different countries to respond to non-compliant behaviour in the same way, avoid e.g. Spain issuing sanctions but Belgium only issuing recommendations

Accountability

- Need to have an internal register to prove that you are doing things in a compliant way
- Should review and update measures, e.g. annual review, legal guidance
- Should take privacy into account when starting projects etc

Control

- Data protection authorities (per country, public, experts, independent)
  - You could be contacted by DPAs outside your country
  - **Complaints can be issued to your own national DPA, against a service in a separate country**

Consent

- Still need **consent for sensitive data**, legitimate interest insufficient
- In a university, as per commercial organisation, students and leaders not balanced relationship so consent is not a valid method
- If you realise you want to use previously collected data for a **separate purpose** that is outside the spirit of the original purpose (e.g. send to 3rd country), ***need*** to get consent (not necessary if data is anonymised)

Sensitive Data

- Special categories, e.g. data that could identify a user as a minority group member, or health related data
- Criminal
- National ID numbers

All of these require a **special legal basis** in place

Purpose of processing

- Must be well defined
- Cannot e.g. share emails outside context to subscribe to a mailing list
  - Now explicitly forbidden by GDPR

Disclosure

- Do I need to disclose the purpose? Yes
- How do you tell people that the purpose or privacy statement has changed? Is this outside purpose? NO – this is **a legal obligation**!
- If email is official communication channel, need to ensure that data protection policy is general enough to cover all use cases
- Overly generic statements will be notified by DPAs and given warnings

Retention

- Need to limit storage time of personal data
- E.g. storing passport copies of old employees from the 90s is not ok
- Should **consider risk of keeping personal data** – the longer you have it the higher the risk. To be able to produce an individual's data within 72 hours should be achievable
- **If you don't need the data, you must not keep it**
- What about logs that you don't know you have? Should at least try to be compliant… probably almost impossible
- Security reasons are allowed as justification for log retention (despite not knowing whether you need specific logs or not), but timeline must be stated.
- Deceased people?

Securing Data

- Responsibility shared between data controller and data processor, both must secure data
- Need to document response procedure for data protection incidents (data breaches)
- **You have an obligation to report Data Breaches to DPAs within 72 hours** – notify as soon as possible, despite not concluding investigations
  - Breaches of encrypted data must be reported if suspicion that the key is known
- When data breach linked to users, they must also be notified
- The same for e.g. loosing a laptop

Individual Rights

- Individuals have a right to **correct** data
- Right to **claim** data (make request)
  - However, not necessarily obliged to delete the data
  - Must **inform** downstream data processors
- Need to have a policy that details how you deal with access requests

Data Sharing

- EU + adequate countries are fine, free data flow (in scope of privacy policy)
- Other countries, previously required
  - Consent
  - Special contractual setup
- **In new GDPR, CoCo is sufficient for transfer to 3rd country**
  - **Valid after CoCo is approved by EC**
  - **Each adoption of CoCo must be registered with DPA (guidelines expected from WP29 but process unclear)**
- GEANT will need to control who can effectively comply with the code of conduct
- Liability rests with the organisation that shared the data to the 3rd party, liability does not rest with GEANT
- 3rd party recipient must deploy safeguards

Presentation Conclusions

- **In context of new GDPR, a CoCo is sufficient for transfer to 3rd country**
- **GEANT will have to manage CoCo adoption**

CoCov2 Walkthrough

- Scoped to cover **necessary attributes** only
- Doc is in keeping with principles of GDPR
  - *BUT* In parallel need to be able to **prove that you are able to comply with GDPR principles**, regardless of adopting the CoCo for all processes not in scope of CoCo
- For IdP/SP Proxies, where the attributes are given to the proxy, the onward flow of attributes is covered by the CoCo

CoCov2 Walkthrough

- Service Provider acts as a data controller
- Purpose restricted to "**enabling access**"
  - Enabling access is split into four parts, including real world trust transfer
  - **Concern that monitoring of usage is not covered, for e.g. security**
- Any data collection or retention outside enabling access requires a separate statement in privacy policy

CoCov2 Walkthrough

- Data minimisation, highlighted those attributes that are appropriate, e.g. unique identifier, name, email (effectively **R&S**)
- Explicitly forbids deviating purposes
  - Q Could consent be used to govern this?
  - Seems to be a logical error in section D stating that consent is the only way to approve a deviating purpose

CoCov2 Walkthrough

- Liability/indemnity (Clause m)
  - ” as determined in a binding and enforceable judicial ruling.” Q: ruling between whom? A: between the HO and the SP.
- Governing law (clause o)
  - ”the country in which the **Service Provider** is established.”
  - Q: What is the governing law if the SP is e.g. in the US?