
CERN

GDPR, e-Privacy, International Collaborations and International Organisations

David Foster
Head of Data Privacy Protection
CERN
April 2017

Agenda

- The following are some initial observations on the GDPR and e-Privacy Regulations.
  - Restricted to a few specific issues for debate.
  - Some focus on uncertainties specific to International Organisations

GDPR and e-Privacy

- The GDPR gives a detailed view of the rights and principles of personal data protection.
  - It is the responsibility of the controller to demonstrate compliance (accountability)
    - They need to be careful who they pass personal data to.
  - International Organisations are specifically ‘third countries’ even if wholly based in the EU and CH.
    - How do they demonstrate adequacy?
- The proposed new e-Privacy regulation strengthens the GDPR in a specific domain, that of electronic communications.
- It is perhaps no surprise that the intention is to have both regulations enforceable on May 25th 2018.
- This is important because it would appear that the provision of services to international collaborations will be subject to both regulations.

International Organisations

- The term ‘International Organisation’ is almost always used in the context of ‘Third countries’ in the GDPR
  - ‘international organisation’ means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries. (Art. 4(26))
- But is it also a Public Body?
  - No definition in the GDPR but a distinction is made with ‘Public Authority’
  - H2020 Guide on beneficiary registration, validation and financial viability check
    - ‘Public body’ means any legal entity established as public body by national law or an international organisation.
  - But several recitals (incl. 93) and Art. 83(7) imply linkage to member state law but do not necessarily preclude public bodies outside member state law.
- Significant implications:
  - If a Public Body then
    - DPO is required (Art. 37(1)(a))
    - Representative in the EU is not required (Art. 27(2)(b) and Recital 80)
  - In not then the converse is true.
    - Who would take on the role of representative in the EU?
      - Liability unclear. “Enforcement proceedings” may be taken against the representative (Recital 80).

Jurisdictional Issues

- Codes of Conduct are one useful mechanism of providing adequate protection (Recital 81)
  - They cover transfers to third countries and international organisations (Art. 40(2)(j))
- The monitoring body verifies compliance (Art. 41)
  - Subject to administrative fines (Art. 83(4)(c))
    - Who will accept these liabilities for scientific collaborations?
  - But public bodies are exempt from monitoring (Art. 41(6))
- Can an international organisation be a signatory to a code of conduct without impact to privileges and immunities?
  - What legal consequence would be applicable?
  - Would a public body label help to avoid legal complexities or weaken provisions?
- Without prejudice to the privileges and immunities, who would be the supervisory body for an international organisation?
  - Is self regulation an option?
  - A formal relationship with the EDPS as for EU institutions?
  - How might ‘adequacy’ be achieved given there is no experience so far?

Proposed e-Privacy Regulation

- "… this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679 …" (Recital 5).
- "This Regulation should apply to providers of electronic communications services, to providers of publicly available directories, and to software providers permitting electronic communications, including the retrieval and presentation of information on the internet …" (Recital 8).
- "… it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications" (Recital 12).
  - An important technical architecture statement.
- " … should not apply to closed groups of end-users such as corporate networks, access to which is limited to members of the corporation." (Recital 13) as explanation of the Article 2(c) exemption which talks of 'public' implying that 'public' should be interpreted broadly as something which is not strictly limited.
- This would appear to bring in scope organisations offering distributed services to international collaborations which cannot reasonably claim the exemption in Article 2(c).
  - Substantiated by the EDPS as examples of 'public' provision of services include "universities to the users of their main services".

Some Observations

- Clarifies the scope of meta-data as personal data.
  - "this Regulation should require providers of electronic communications services to obtain end-users' consent to process electronic communications metadata" (Recital 17) clarifying Article 6(2) for all processing other than that strictly necessary.
    - "For the purposes of this Regulation, consent of an end-user, regardless of whether the latter is a natural or a legal person, should have the same meaning and be subject to the same conditions as the data subject's consent under Regulation (EU) 2016/679." (Recital 18)
    - Does this mean for Codes of Conduct are not sufficient as a legal basis for processing, for example, AAI attributes? Possibly not, given:
      - metadata is "any data that is processed by any other equipment for the provision of the service and which is not considered content" as clarified by the EDPS.
      - But "user's consent to the processing could be expressed by using the appropriate settings of a browser or another application." as welcomed by the EDPS.
        - But how "freely given" is it in the employer/employee context?
- This regulation also requires a "representative in the Union" where the provider is not established in the Union. (Article 3(2))
  - As this particularises the GDPR then this appears to be requiring international institutions (including International Organisations) who provide distributed computing services to have a representative in the Union.
    - e.g US universities and labs?

Conclusions

- With the good intentions of ensuring adequate protection of personal data the immediate organisational objective is to reduce risk of non-compliance.
  - But there is much ambiguity concerning International Organisations and jurisdictional issues.
  - How will International Organisations operate as part of global scientific collaborations practically?
- It would seem imperative to look at the two regulations together when determining compliance strategy for distributed systems and services (e.g EOSC)
  - The e-Privacy regulation influences all types distributed systems as part of global computing services and scientific collaborations.
  - Codes of conduct may not be complete solutions.
  - “Representative in the Union” needs much more clarification as to implementation.
- Much more communication is needed to avoid the major pitfalls and justify interpretation even if legal clarity will only come much later.
  - GDPR Art. 50 on international cooperation has many good intentions but needs to be engaged now.
- What will happen on May 25th 2018 given such uncertainties and the strong stance of the EC and the regulators?
  - There needs to be dedicated consultation with the international scientific community and time for the adaptation of existing global services.