Epic fails and good practices in the quest for GDPR compliance

by Cristina DeLisle, XWiki SAS
A few words about me @ XWiki SAS

- DPO of XWiki SAS, an Open Source company
- XWiki & Cryptpad: Open Source projects
- Our privacy compliance journey
Transversal impacts of the GDPR

- **Legal and compliance governance:** privacy strategies, accountability, lawfulness, policy making, auditing

- **Data collection and lifecycle:** purpose limitation, data minimization, transparency

- **Tech:** data breaches handling, encryption solutions, privacy by design & default
Epicly failing to comply: areas of biggest fines so far

• Coerced consent from data subjects

• Data security areas:
  – Leaks
  – Breaches of confidentiality, availability, integrity

• Cyber Attacks

63,437 security incidents¹
1,367 confirmed data breaches¹
1 in 3 documented data breaches occurred in businesses with under 100 employees⁷
60% of small businesses close their doors within half a-year of being victimized by a “cybercrime”⁹
Article 42 EU GDPR
"Certification"

The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.
Standardization (so far) only as a best practice

- ISS & data protection: procedures, products, management systems, organizations, individuals
- FLSC
- Certification under French decree No. 2002-535
- ISO-27001
- ISS certification of individuals: CISSP, CISM, ISO 27001 Lead Auditor, IAPP
- International standards, guides published by institutions: CNIL, ANSSI
Tools / Further readings

- General Security Framework (RGS): "Adapting ISS to the issues at stake", "Using products and providers awarded with security certification", "Efforts commensurate with ISS stakes"

- RGS and the associated appendices: "Acknowledging registration and acknowledging receipt"

- Catalogues of products recognized by ANSSI

- ANSSI SSI Maturity and ANSSI GISSIP guides
OSS & the GDPR

- **OSS Licences**: LGPL, MIT, Apache etc.
- **Control of the downloaded OSS**: data to the people
- **The community & the infrastructure provider**
- **Cloud computing** hosting company compliance
- **Extraterritoriality** of the GDPR
OSS & the GDPR

• OSS governance is by default:
  – Transparent
  – Privacy oriented: for the people, by the people
  – Facilitating meritocracy

• OSS innovation & privacy
  – Decentralization
  – Federation networks
  – Zero knowledge collaboration software
Feel free to contact me!

- cristina.rosu@xwiki.com
- @cristina.r:matrix.org
- @redchrision@mastodon.social
- XWiki POSS 2018 stand