Open source in the quest for GDPR compliance

by Cristina DeLisle, XWiki / Cryptpad

FOSDEM 2019

A few words about me @ XWiki

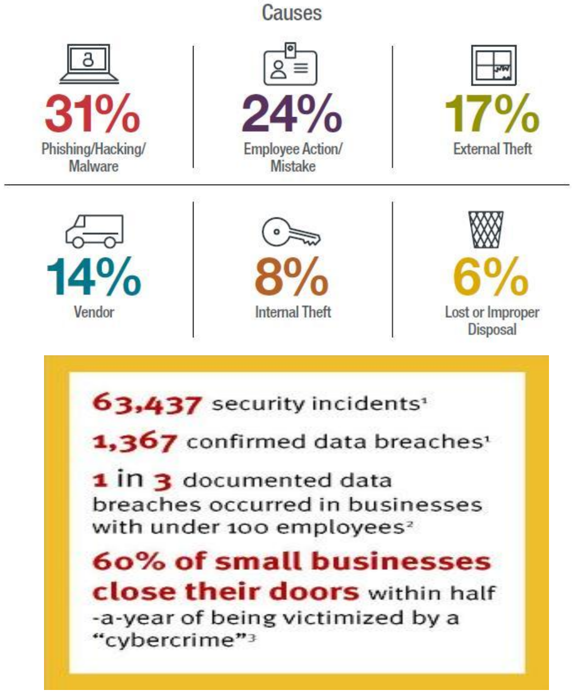
- **DPO of XWiki SAS**, Top sponsoring company of:
  - XWiki & Cryptpad: Open Source projects
- **Our privacy compliance journey**

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

Areas of biggest fines so far

- **Coerced consent** from data subjects
- **Data security areas:**
  - Leaks
  - Breaches of confidentiality, availability, integrity
- **InfoSec**



Causes

31% Phishing/Hacking/ Malware

24% Employee Action/ Mistake

17% External Theft

14% Vendor

8% Internal Theft

6% Lost or Improper Disposal

63,437 security incidents[1]

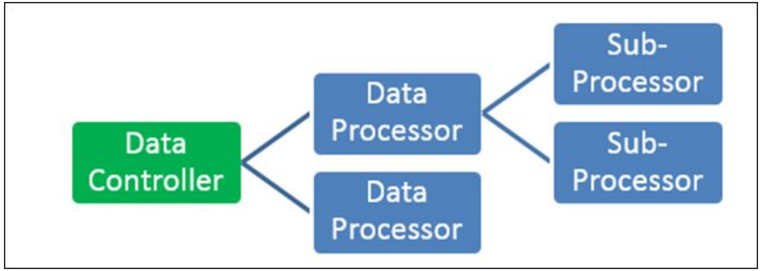
1,367 confirmed data breaches[1]

1 in 3 documented data breaches occurred in businesses with under 100 employees[2]

60% of small businesses close their doors within half -a-year of being victimized by a "cybercrime"[3]

The model of controllers & processors

- **Controller:**
  - company who determines the purpose and means of processing



- **Processor:**
  - third party that processes it on a controller’s behalf
- **Data processor agreement (DPA)**
  - You can act as a controller & processor at the same time, depending on how the personal data gets handled

Data controllers & processors

- **2012:** Google Inc. as a controller, under Directive 95/46/EC
  - ECJ on Google Sp & Google Inc vs. Mr. Gonzales
- **By 2016:** Google received 347,533 separate requests to remove aprox. 1.2 million websites

The OSS model

- **The OSS community**
  - Data subjects
  - Enforced rights on their personal data

- **The “infrastructure providers”**
  - Controllers & Processors

Illustrations of who’s who

- **XWIKI OSS:**
    - Controller of hosting for xwiki.org: XWiki SAS
    - Processor: OVH

- **Github (<3 OSS):**
    - Controller of the PD from your free private user account
    - Processor of your invoices

Lawful reasons for processing PD

- **Compliance with the law**
  - legal obligation

- **Legitimate interest**
  - vs. the data subject’s interests
  - “careful assessment”

- **Contract**
  - with the data subject

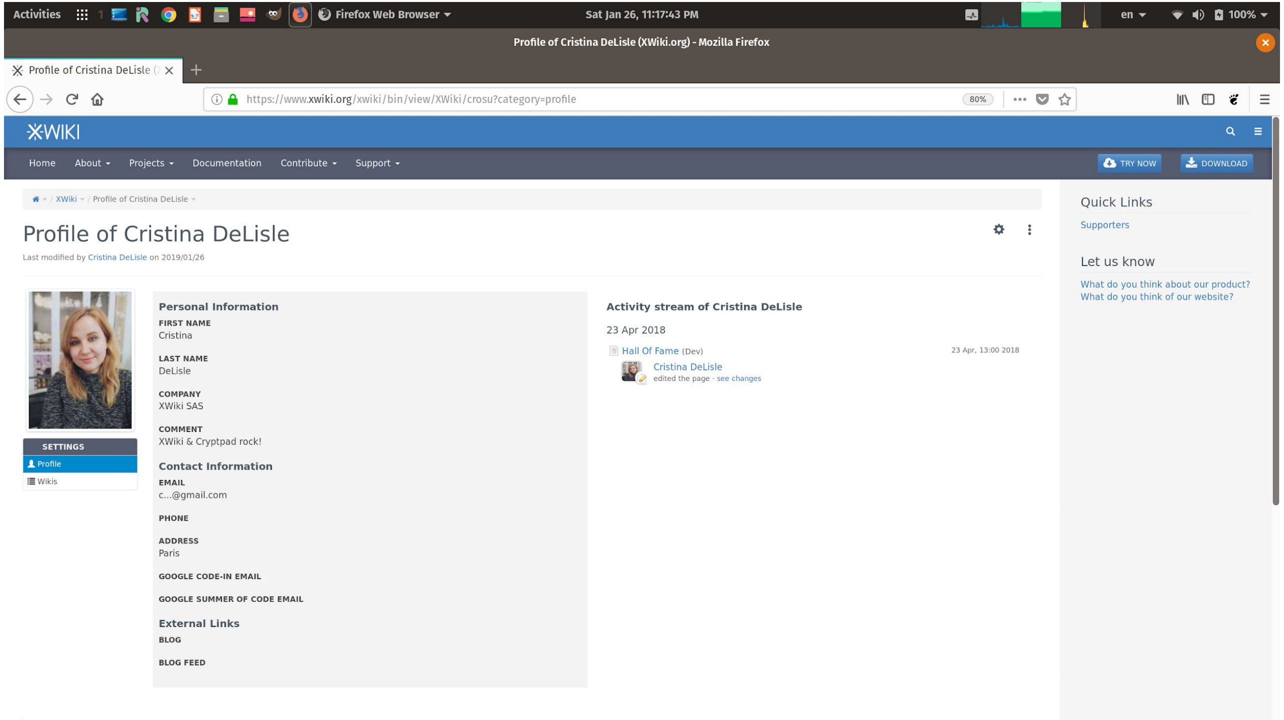
- **Consent:**
  - specific & informed
  - affirmative action
  - freely revocable

Contract

- **Your user name & email address**
  - given in order to create your Github account

- **Terms of Service agreement** with Github

Consent


Activities
Firefox Web Browser
Sat Jan 26, 11:17:43 PM
en
100%
Profile of Cristina DeLisle (XWiki.org) - Mozilla Firefox
Profile of Cristina DeLisle (
https://www.xwiki.org/xwiki/bin/view/XWiki/crosu?category=profile
80%
XWIKI
Home
About
Projects
Documentation
Contribute
Support
TRY NOW
DOWNLOAD
XWiki / Profile of Cristina DeLisle
SETTINGS
Profile
Wikis

Profile of Cristina DeLisle

Last modified by Cristina DeLisle on 2019/01/26

Personal Information

FIRST NAME
Cristina

LAST NAME
DeLisle

COMPANY
XWiki SAS

COMMENT
XWiki & Cryptpad rock!

Contact Information

EMAIL
c...@gmail.com

PHONE

ADDRESS
Paris

GOOGLE CODE-IN EMAIL

GOOGLE SUMMER OF CODE EMAIL

External Links

BLOG

BLOG FEED

Activity stream of Cristina DeLisle

23 Apr 2018

Hall Of Fame (Dev) 23 Apr, 13:00 2018
Cristina DeLisle
edited the page · see changes

Quick Links

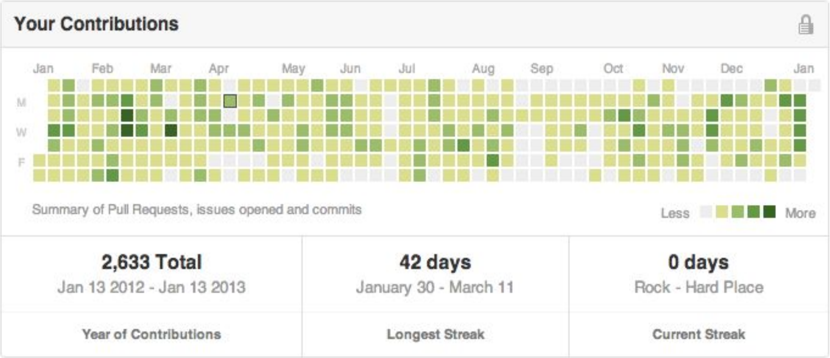
Supporters

Let us know

What do you think about our product?
What do you think of our website?

Legitimate interest

- **Commits to the source code of an OS project**
  - Name & email



Your Contributions

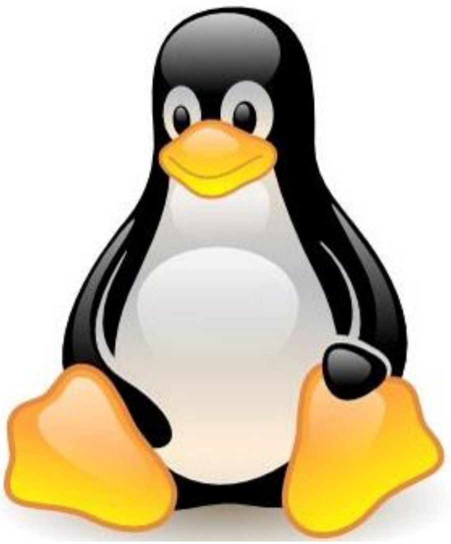
Summary of Pull Requests, issues opened and commits

2,633 Total	42 days	0 days
Jan 13 2012 - Jan 13 2013	January 30 - March 11	Rock - Hard Place
Year of Contributions	Longest Streak	Current Streak

Developer Certificate of Origin (Linux)

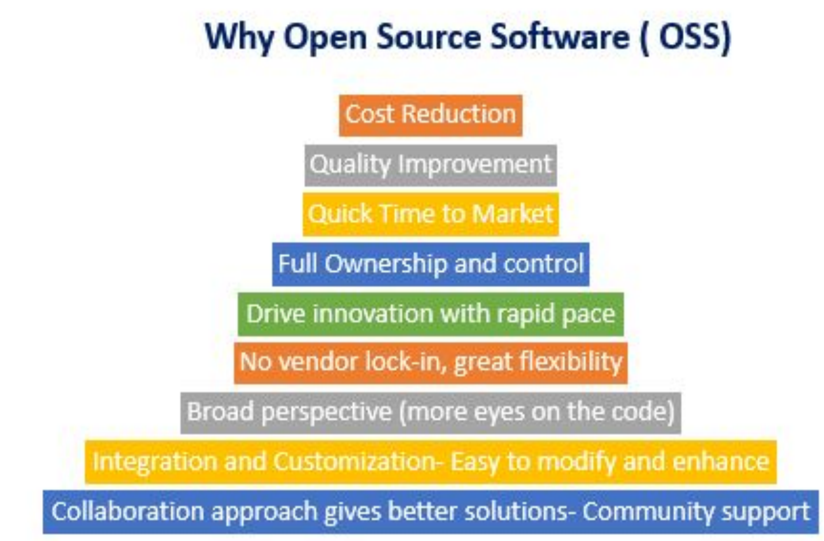
By making a contribution to this project, I certify that: (...)

(d) I understand and agree that this project and the contribution are public and that a record of the contribution (**including all personal information I submit with it, including my sign-off**) is maintained indefinitely and may be redistributed consistent with this project or the open source license(s) involved.



OSS & the GDPR

- **Control of the downloaded OSS:** data to the people
- **Cloud computing** hosting company compliance
- **Extraterritoriality** of the GDPR



Why Open Source Software (OSS)

Cost Reduction

Quality Improvement

Quick Time to Market

Full Ownership and control

Drive innovation with rapid pace

No vendor lock-in, great flexibility

Broad perspective (more eyes on the code)

Integration and Customization- Easy to modify and enhance

Collaboration approach gives better solutions- Community support

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

Cryptpad: Privacy by design & default

- **By design:** technical and organizational measures such as encryption in place, to minimize personal data processing
  - **“zero knowledge” collaborative software**

- **By default:** only process data that is necessary, to an extent that is necessary, as long as necessary.
  - **encrypted editors in the Cloud**

Feel free to contact me!

- cristina.rosu@xwiki.com
- @cristina.r:matrix.org
- @redchrision@mastodon.social
- XWiki FOSDEM 2019 stand