General Data Protection Regulation

For BOINC Projects

Shawn Kwang
University Wisconsin-Milwaukee
Einstein@Home

This presentation

Link to slides only: https://tinyurl.com/yad2m7uv

Introduction and overview

- GDPR and BOINC
  - When: **Friday 2018 May 25**
  - Who: Affects any BOINC project whose volunteers are EU citizens.
  - What: the meat of this talk
  - Why: should I care?
- Who: GDPR affects a project if
  - data controller, or processor, or the data subject is based in the EU.
    - controller: an organization that collects data from EU residents
    - processor: an organization that processes data on behalf of a data controller
    - data subject: anyone from the EU.
  - The regulation also applies to organisations based outside the EU if they collect or process personal data of individuals located inside the EU.
- Summary: We BOINC projects are 'controllers' (and processors) and our volunteers are 'data subjects'

What is personal data?

Any information related to 'data subject', that can be used to directly or indirectly identify the person.

"It can be anything from a <u>name</u>, a photo, an <u>email address</u>, bank details, posts on social networking websites, medical information, or a <u>computer's IP address</u>."

- I've underlined the items which all BOINC projects automatically collect by default.
- If your project, like Einstein@Home, has forums and other social elements, these are personal data as well.

Core concepts (the "what")

1. Project's Terms of Use.
2. User Opt-in - consent to project's terms of use.
3. User Right-of-access - obtaining user's own data.
4. User Right-of-erasure - deleting a user's account.
5. Data protection by design and default.

#1 Projects must document what personal data is collected. Projects must specify what they will do with a user's data and who they will share it with, e.g., BOINCstats.

#2 Consent

- Volunteers must explicitly give consent to data being collected.
- We as projects must be able to prove this consent.
- And the consent may be withdrawn.

Links:

- https://boinc.berkeley.edu/trac/wiki/UserOptInConsent
- https://github.com/BOINC/boinc/issues/2413

#3 Right of access

- Users have the right to access their personal data and be given information about how their data is being used.
- Projects must provide an overview of the categories of personal data stored.
- Projects must also provide the data itself, in a portable format.

#4 Right of erasure

- Users may request deletion of all personal data.
- What gets deleted?
  - Technical: This also means deleting records associated with a user, such as user's host(s).
  - IBM/WCG developed two 'delete' functions: one less strict (default) and one more strict.
- As of May 2018 this code is in the BOINC master branch.

Links

- https://boinc.berkeley.edu/trac/wiki/RightToErasure
- https://github.com/BOINC/boinc/issues/2447

#5 Privacy by default

Projects should set their privacy related settings at a high level by default.

- Example: show_hosts flag in user table, should default to false.

Links

- https://github.com/BOINC/boinc/issues/2449

Conclusion

Why should I care?

- Projects based in Europe will be subject to sanctions.
- Projects based elsewhere may be subject to judicial action as well.

As with any new law, going forward, there will be much decided by judicial rulings and court cases!