GDPR and the Canadian Research Landscape

JAMES MACGREGOR, PKP

FOR RDC / DRC

JUNE 28, 2018

Webinar Recording Policy / Politique concernant l'enregistrement des webinaires

This webinar will be recorded and archived, including all audio. The video will be archived on the CANARIE YouTube channel and may be promoted through RDC and/or CANARIE communication channels.

Any text questions or comments, if responded to, will remain anonymous and not be part of the recording. The recorded video will include your voice, if audio participation is enabled.

Ce webinaire sera enregistré puis archivé, son compris. La vidéo sera conservée sur le canal YouTube de CANARIE et pourra être promue au moyen des filières de communication de DRC et de CANARIE.

Si on y répond, les questions écrites et orales demeureront anonymes et ne feront pas partie de l'enregistrement. Toutefois, si la fonction « participation audio » a été activée, le fichier vidéo inclura votre voix.

The PKP-GDPR Team

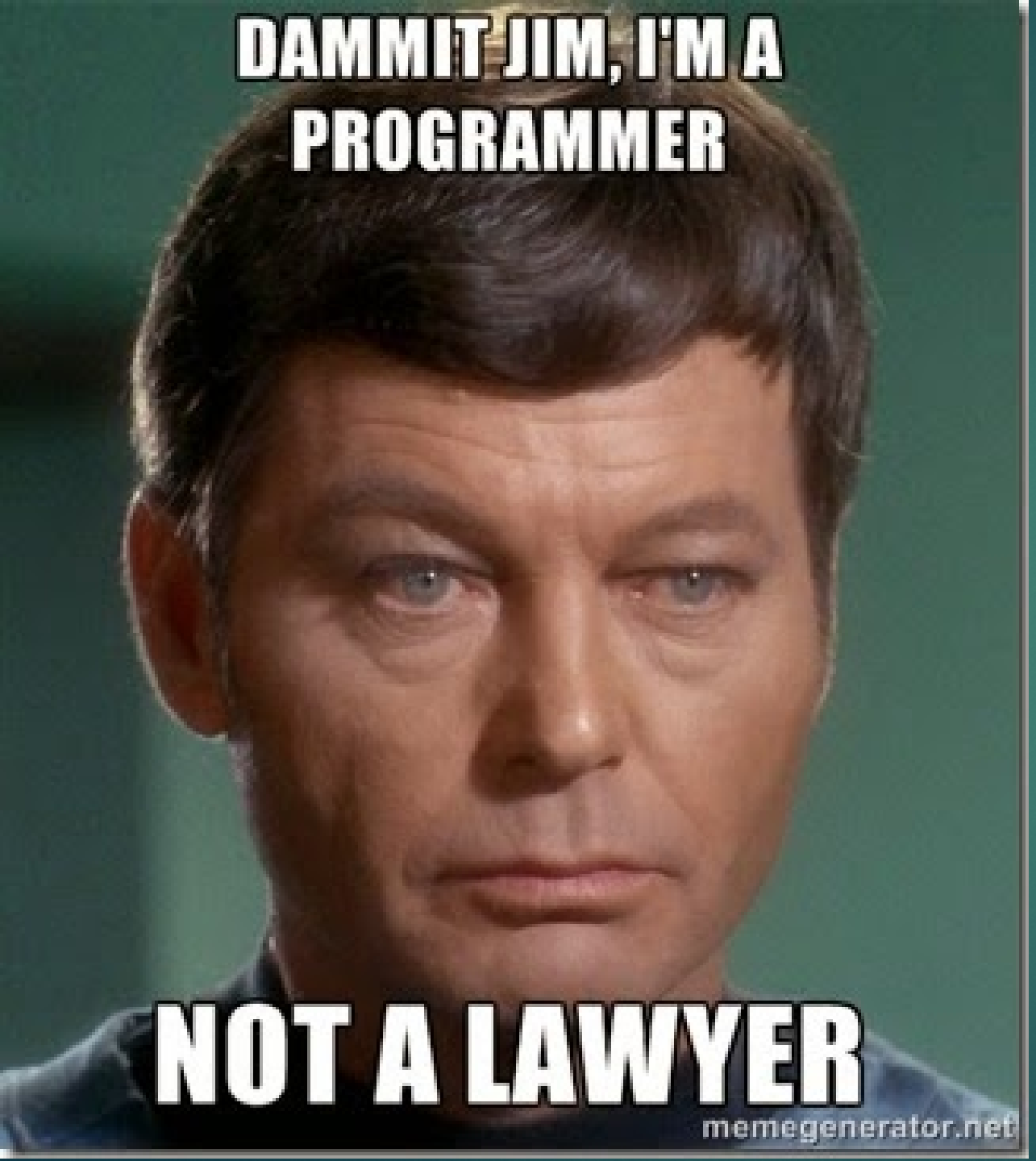
Multiple individuals and organizations played a significant role in developing our understanding of and approach to GDPR, from policy practices to technical requirements:

- Development Partners in the EU (journal.fi; Free University Berlin; Heidelberg University)
- Hosted clients
- General community members, on the PKP Forum (https://forum.pkp.sfu.ca) and on Github (https://github.com/pkp)

The PKP-GDPR Team

This distributed, decentralized and cooperative team assisted with the following:

- Understanding the GDPR (esp. from an EU perspective)
- Scoping the technical challenges (bug entries, feature requests)
- Reading, writing and reviewing documentation / guidelines
- Limited legal review (country-specific)
- Code contributions



Who am I?

- PKP Associate Director of Strategic Projects and Services
- 10+ years of scholarly publishing experience
- In charge of our Publishing Services hosting initiatives
- Coordinated the GDPR Team
- Not a lawyer!
- (Also technically not a programmer)

One more note before we begin:

PKP's understanding of GDPR has been iterative, and will continue to improve over time. This can probably be said of everyone's understanding, and is a common refrain we hear in other communities.

1/3: What is the GDPR?

What is the GDPR?

- **General Data Protection Regulation (GDPR):** The EU's regulations for the handling of personal data on the Internet by service providers. The GDPR defines the responsibilities that **Data Controllers** and **Data Processors** must adhere to with respect to the collection, processing, storage and destruction of any **Personally Identifying Data** that can identify a **Data Subject**.

What is the GDPR?

In my mind, GDPR is a **common-sense** data privacy regulation. Most simply put, organizations should take care to always have a legal basis for processing private information; individuals should always know how their information is being processed; and individuals should (almost) always have a say about how and whether their data is processed.

Who does this concern?

- **Data Controller**: the entity that dictates the terms for processing data. With respect to PKP applications, this would be the editorial management team.
- **Data Processor**: the entity that manages all processing of the data on behalf of the controller - typically the journal, conference or press manager in combination with any systems administrators and service providers.
- **Data Subject**: a natural person whose personally identifying information may be tracked within a given system.

What are the Data Subject Rights?

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object;
- the right not to be subject to automated decision-making including profiling.

What are the Data Subject Rights?

In order to adhere to the GDPR, people acting in the role of **data controller**, in conjunction with those serving as a **data processor**, must provide adequate means for **data subjects** to assert these rights.

What is being protected?

- **Personally Identifying Information** (PII), or **Personal Data**: any information that can potentially be used to identify a person, such as: their name(s); email address; mailing address; phone number; social network posts; or an IP address.

What is exempted?

- Some rights (eg. the right to erasure) are exempted if the personally identifying information is **journalistic** or **scholarly** in nature, or otherwise in the public interest.

What is exempted?

- Scholarly and research data falls within what the GDPR recognizes as a need “to reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression” (GDPR, Article 85)
- In scholarly publishing, data concerning the authors, editors, reviewers, and others involved in the editorial and publishing process remains necessary for the purposes of the journal or press, and, as such, forms part of a record that the GDPR allows “for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes the preservation of which is in the public interest” (Recital 65).

A note on consent

To process private data, you need a **lawful Basis for Processing Personal Data**: the basis by which a data controller must explain their ability to process data. The most common lawful basis is by **consent,** the agreement of a data subject to share personal data.

In order to satisfy GDPR, consent must be unambiguous (and in the case of sensitive personal data must be explicit, i.e. “opt-in”), and must be able to be withdrawn.

2/3: How do I comply?

How do I comply?

1. Establish your role. Are you a Data Processor, or a Data Controller? (PKP is both, depending on context.)

How do I comply?

2. Review your system and establish:
    1. What PII you collect
    2. How it is processed
    3. How it is stored
    4. How it is protected
    5. That you have a legal basis by which to request and process said data

How do I comply?

3. Protect your data, and reduce your collection footprint.
   - Establish **and document** secure data management practices
   - Encrypt what you can
   - Don’t collect data you don’t need
   - Only store data for as long as required

How do I comply?

3. Develop and provide adequate privacy processes and rules

- Write and publish a privacy policy:
  - Data Subjects must know what data you collect
- Establish a means of contact and a Data Privacy Officer:
  - Data Subjects must have an opportunity to enforce their rights
- If you develop and application or platform, understand and follow **privacy by design**
- If you are a service provider, you must have documented processes in place for eg. **privacy breach notifications**

How do I comply?

4. Integrate continuous review into your practices
   - Compliance isn’t a one-off thing.
   - Systems and processing workflows must be routinely reviewed, good development practices must be adhered to.

3/3: An example of our process in action

Cookies

Cookies have received a lot of attention lately, and everyone seems to have a new cookie popup warning. **Are they necessary?**

- GDPR doesn't say anything about cookies. It's only concerned with individual privacy.
- There is a difference between session and tracking cookies.
- A session cookie maintains state (used for website logins, etc.), and doesn't normally contain PII.
- A tracking cookie can user behavior against IP addresses, and contains PII.
- PKP's policy: no need to mention the OJS session cookie. But if Google Analytics or another tracking script is used, that needs to be accounted for.

Thank You! Questions?

James MacGregor

Public Knowledge project

Email: james_macgregor@sfu.ca

Twitter: @jmacgreg

Resources

EU GDPR Information Portal: https://www.eugdpr.org/

PKP GDPR Guide: https://pkp.sfu.ca/2018/04/30/gdpr-guidebook-pkp/

Project on Github: https://github.com/pkp/pkp-lib/projects/11

The main GDPR forum thread: https://forum.pkp.sfu.ca/t/is-ojs-gdpr-compliant/37521