Understanding GDPR
Libraries, Repositories, & Privacy Policies

JENELYS COX, MLIS

INSTITUTIONAL REPOSITORY MANAGER
& APPLICATION SUPPORT TECHNICIAN

UNIVERSITY OF DENVER

What is GDPR?

- EU General Data Protection Regulation (EU-GDPR)
- A European Union data privacy act
  - Went into effect May 25, 2018
  - Update to the 1995 Data Protection Directive (*Directive 95/46/EC*)
- Goals
  - Modernization of data privacy regulations
  - Standardization of data privacy regulations across the EU
  - Address privacy at the design phase, rather than as an afterthought
- Available at: http://www.privacy-regulation.eu/en/index.htm

What does GDPR do?

- Defines personal data (any relating to ID'd or ID-able person)
  - Financial, demographics, communication records, contact info, ID #'s, IP address, etc.
- Requires "controllers" and "processors" to follow specific regulations when collecting and storing personally identifiable data on "subjects"
  - Controllers & processors
    - Collect, store, & transmit personal data
    - Service providers
  - Subjects
    - Identifiable individuals whose data is collected, stored, or transmitted
    - Service users
- Assigns rights to "subjects" over their own data
- Applies when controller, processor, OR subject is in the EU

What does GDPR require?

- Data Privacy Register
  - A record of data collection & processing which must include
    - Purpose of collecting/storing data
    - Type of data
    - Who receives the data
    - Security info on the process & storage
- Subjects have certain rights over their personal data
  - Right to request access to their stored records
  - Right to correct the record
  - Right to remove their record (within reason)
  - Right to transfer their record
- Privacy demonstrably addressed during design
- Subject consent to collect data
  - Subject must be informed of data collected and willingly agree
- Privacy policy
  - The information provided to subject, which must include
    - Data collected
    - Contact info for subjects to request records, changes, removal, or transfer of data
    - Statement of security protocols
- Security protocols
- Procedures for breaches of security which must go into effect w/in 72hrs of discovery

Scope of GDPR

ARTICLE 3

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
    a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
    b. the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

See http://www.privacy-regulation.eu/en/article-3-territorial-scope-GDPR.htm

So, does this actually affect our IRs?

From bepress's perspective

- Business w/ goal of selling their product to EU subjects
- Elsevier based in Amsterdam & thus subject to the full extent of GDPR
  - Bepress as a subsidiary is also required to comply

From the library perspective

- Not really
- Non-profit, not selling products
- Not tracking behavior for the purpose of targeted advertising or similar marketing purposes
- May differ at the University level

Chapo, R. A. (2018) The Scope of GDPR. https://www.socalinternetlawyer.com/territorial-scope-gdpr/

Where We Are @ DU

- Campus IT has been looking into GDPR compliance
  - Evaluating vendor products
  - Evaluating & updating home-grown products
  - Full GDPR compliance
- Library has just finished round 1
  - Formed a task force
  - Performed basic data audit
  - Rewrote our privacy policies to be easily accessible & understandable
  - Not full GDPR compliance

Considerations

Why are we doing this?

- Standardization
  - GDPR provides guidelines
- Risk management
  - Pathways for security
  - Less data to lose
- Build trust
  - Show our patrons we care

What are we addressing?

- Transparency
  - Do patrons know we have data?
- Autonomy
  - Can patrons choose what data they give us?
- Security
  - Are the platforms we're using adequate to protect patron privacy?

How do we address it?

- What do we collect?
  - Patron accounts
  - Proxies, websites, chat records, & logs
  - Usability, student success, & library use
- Why do we collect it?
  - Necessary for operation
  - "Improving Services"
- Is it justified?
  - Do we *actually* need it?
  - Do we need to *keep* it? How long?

Privacy Policies

Addressing Transparency

- State what we collect, why, and how long we keep it
- State what our policy covers
  - Make it obvious we don't control our vendors

Addressing Autonomy

- If data is not necessary to basic operation, allow opt-in/out
  - Easy & obvious for the patron, with an explanation of what may be affected
  - May require scripts, workarounds, or recoding
  - Not yet in place

Addressing Security

- Have a stated procedure for breaches
  - Contact all appropriate parties (Patron, Campus IT Security, Vendor, Others)
- In place, not yet explicitly stated

DU's Privacy Policy (Pt 1)

work in progress

The Basics: What our policy covers & why.

- The University of Denver Libraries are deeply committed to protecting the privacy of the students, faculty, staff, and visitors we serve. We are guided by the American Library Association's Code of Ethics, which states, in part, that "we protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted," and that "we do not advance private interests at the expense of library users, colleagues, or our employing institutions." We firmly believe this right to privacy is a fundamental condition to intellectual freedom and the pursuit of knowledge.
- When you use our services, however, you generate data. We may collect and analyze these data in order to improve our services in the pursuit of supporting your success. We make every reasonable effort to anonymize and protect these data, and consider them an institutional asset subject to the University of Denver's Privacy Statement.
- It is important to understand that modern library systems are complex and we license content and services from third-party vendors who have their own privacy and confidentiality practices. While we make every reasonable effort to hold all our licensed services to the same standards, and attempt to send as few personal identifiers as possible when connecting users to a resource, some information is required for authentication, troubleshooting, or customized services. We encourage you to review the privacy and confidentiality policies of these parties.

DU's Privacy Policy (Pt 2)

work in progress

Providing Autonomy: How to contact us.

- Below are the types of data you may generate when you use our systems and services, and what we do with them. If you have questions about your privacy as it relates to these data and this statement, please feel free to contact the University Libraries Dean's Office.

DU's Privacy Policy (Pt 3)

work in progress

Transparency: LMS & ILL

- When you check out print materials:
- Data are stored in our library management system for the purpose of managing patron accounts and providing services. Access to these data are restricted to library staff and faculty. Examples of data in this system include:
- * Your name, address, phone, email and ID number.
- * The items you currently have checked out or requested.
- * The items you previously checked out that still carry a fine.
- * The items you have requested through Interlibrary Loan.
- Once you return an item, and you do not owe a fine on the item, your checkout of the item is anonymized and the item cannot be traced back to you. If you borrow materials from other institutions through Interlibrary Loan, records of these transactions are stored in a separate internal system and not automatically anonymized. Your name and the item you request is transmitted to the lending library. Please contact Interlibrary Loan if you would like to know more.

DU's Privacy Policy (Pt 4)

work in progress

Transparency: Our physical spaces

- When you use our facilities:
- We collect data regarding how many people enter/exit the building and peoples' usage of space during library operating hours. These data are anonymized. They are used to improve the design of physical space within the building.
- When you use our walk-in services, at desks or in instruction rooms:
- We may collect e-mail addresses and other contact information, in order to provide and improve our services. Special Collections and Archives researchers are required to complete a registration form prior to using collection materials in the Reading Room. Identifying information (mailing and e-mail address, other contact information) is recorded on this form. The forms are held on paper in Special Collections for a period not to exceed three years from the date of last visit. Visitors are only requested to complete the form if Special Collections and Archives does not already have their information on file.

DU's Privacy Policy (Pt 5)

work in progress

Transparency: Our online catalog

When you use Compass, our catalog and discovery tool:

Data are gathered and made available to the Libraries that includes operating system, browser, country, on or off-campus location, whether or not a user is signed into their library account, searches performed, and site navigation. No personal information is made available to the Libraries. This tool is contracted through ExLibris. Additional information about the data collected by ExLibris can be found at: https://www.exlibrisgroup.com/privacy-policy/

DU's Privacy Policy (Pt 6)

work in progress

Transparency: Our websites

When you use any portion of our website:

The Libraries' website, research guides, A-Z database list, Special Collections@DU, Special Collections and Archives catalog, Digital Commons, and Yewno are tracked using Google Analytics. Data gathered include the browser, operating system, and city of the device being used, searches performed, and site navigation. The Libraries do not use Google Advertising Features, so no personal or demographic data are made available to the Libraries via Analytics. However, if you are logged into your Google Account while using the Libraries' website or tools, additional data may be tracked and linked to your Google Account. Additional information, including instructions on adjusting what data Google connects to your account, can be found at: https://myaccount.google.com/privacy Google also offers a browser add-on that allows you to opt out of Google Analytics: https://tools.google.com/dlpage/gaoptout

Springshare (research guides and A-Z database list), Digital Commons, and Yewno are tools provided by third-party vendors. These vendors may or may not capture additional data. Their privacy policies can be found at the links below: o https://www.yewno.com/privacy o https://www.elsevier.com/legal/privacy-policy o https://springshare.com/privacy.html

DU's Privacy Policy (Pt 7)

work in progress

Transparency: Our databases

- When you log-in using your campus credentials for databases:
- Our authentication technology, EZProxy, is hosted by OCLC, a non-profit library cooperative, and collects anonymized data (randomized sessionID and timestamp), as well as the resource accessed. A separate log includes your username, the sessionID and timestamp, but not the resource accessed. We may use these logs to troubleshoot authentication errors or prevent and/or stop security breaches when they occur. We may also anonymize and analyze these logs in order to assess our collections and their use.
- Please see OCLC's hosted services page for more information: https://www.oclc.org/en/policies/privacy.html#hosted-services.
- Once you are authenticated, none of these data are passed on to the third-party database provider. We license many hundreds of these databases in support of your scholarship, so there are too many to provide here. We encourage you to review privacy policies for these vendors.

DU's Privacy Policy (Pt 8)

work in progress

Transparency: Release to Law Enforcement

- Release of information to law enforcement officials:
- The University Libraries will only release Library patron information if legally mandated by law enforcement investigators with an appropriate warrant, subpoena, or court order. In October, 2001, Congress passed the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" (USA PATRIOT Act) which broadly expands law enforcement's surveillance and investigative powers. More about this Act can be found at the American Library Association USA PATRIOT Act and Intellectual Freedom.
- University Libraries does not keep extensive records on individual patrons, but in the event of a valid court order the following information would be available to law enforcement:
  * The patron's record that includes information like name, address, phone, email, and ID number.
  * Any items a patron currently has checked out or requested.
  * Any reading history a patron chooses to save.
  * Any items a patron had checked out that still carry unpaid fines.
  * The last (most recent) patron who checked out an individual item.
  * The patron's record of Interlibrary Loan requests

Thank you! Questions?

JENELYS COX

JENNIFER.COX@DU.EDU