LIBRARY FREEDOM PROJECT

QUESTIONS ABOUT VENDOR PRIVACY PRACTICES

Libraries consider privacy one of our most important core values, and our vendors also have a duty to uphold these values. We've created this resource of questions to ask your vendors about their privacy practices to help hold them accountable to our core values.

These questions were adapted from the NISO Privacy Principles, a consensus agreement between librarians and library content and software providers on best practices for protecting library patron privacy.

Is the vendor familiar with the NISO Privacy Principles? Was the vendor involved in the creation of the principles? Vendors who created the principles:

- Elsevier (RELX)
- ProQuest (Clarivate)
- The Galecia Group
- EBSCO Information Services
- The Cherry Hill Company
- OCLC
- Ex Libris Group
- ITHAKA
- University of Oxford Press

NISO Privacy Principles
https://groups.niso.org/higherlogic/ws/public/download/16064/NISO%20Privacy%20Principles.pdf

Is the vendor familiar with our ethical (and in some cases legal) obligations to preserve patron privacy and prevent unauthorized collection, use, or disclosure of library users' data? Documents to reference:

- **ALA Code of Ethics** http://www.ala.org/advocacy/proethics/codeofethics/codeethics
- **State library patron privacy laws (US)** https://www.ala.org/advocacy/privacy/statelaws

Has the vendor made available to library users specific, non-technical statements that describe the policies and practices relating to the management of personally identifiable information? Do these statements identify:

- what data is collected
- why data is collected
- who has access to the data
- how the data is stored and secured (continued on back)
- when that data might be disclosed and to whom
- and what the organization's data retention and/or deletion policies are?

	Is the vendor compliant with current information security best practices? This includes ○ encryption of personal data while at-rest and in-motion ○ prompt updates of systems and software to address vulnerabilities ○ systems, procedures, and policies for access control of sensitive data ○ a procedure for security training for those with access to data ○ documented procedures for breach reporting, incident response, and system, software, and network security configuration and auditing.
	Is the vendor collecting personally identifiable information (PII)? Is that data collection for purposes other than supporting user services, research to improve those services, or for the internal operations of the vendor for which the data was gathered? Was this collection disclosed to the library user, and did the user consent?
	Is PII being anonymized?
	Was the library user informed about how much PII is collected from them and how it may be used? Is the default setting that users are opted out of data collection unless they explicitly choose to opt in?
	Is the vendor sharing data with third parties, and if so, what third parties, and for what purposes?
	Have the vendor's privacy policies and practices been made easily available and understandable to library users?
	Does the vendor support anonymous use of their products? If not all service capabilities may be available while a user remains anonymous, has the vendor created reasonable accommodations for anonymous users?
	Do library users have the ability to access their own personal information or activity data? Can they delete their data upon request?
	Does the library vendor continuously assess and strive to improve user privacy as threats, technology, legal frameworks, business practices and user expectations of privacy evolve?
	Are the vendor's privacy practices and policies reviewed and reported periodically?

INSTITUTE of Museum and Library SERVICES

We created this resource thanks
to the support of our sponsor.