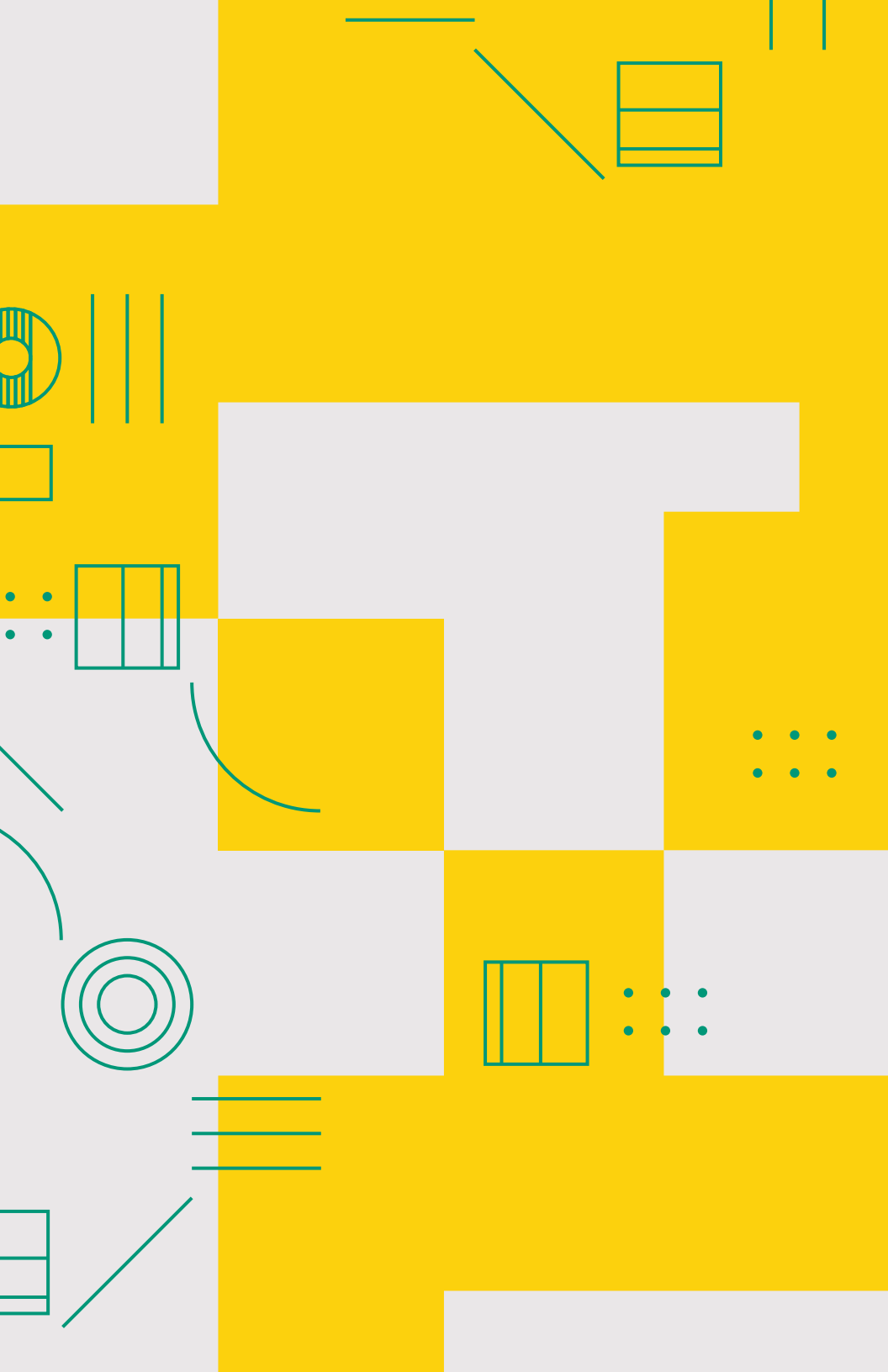


Vendors help libraries serve users by providing critical infrastructure products and electronic resources. Libraries increasingly depend on vendors for these products and resources, but at what cost to user privacy? This guide will introduce you to methods to protect users' privacy while evaluating and acquiring products and resources from vendors. The guide will cover key strategies that libraries can employ to protect user privacy: contract language and negotiations, Requests for Proposal (RFPs), and vendor audits.

However, not all libraries have control over the vendor acquisition process. If the decision making is out of your hands, this guide can still help in identifying strategies to convince the decision makers to keep user privacy in mind during the acquisition process.

Who Controls the Decision to Buy?

Institutions have a wide range of purchasing processes. Some library workers have sole discretionary power over acquisition of vendor electronic resources or software

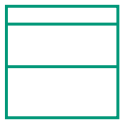
If you purchase, or have access to vendor products through a consortium, ask the consortium what their privacy policy is and what standards they hold vendors to during the acquisition process.

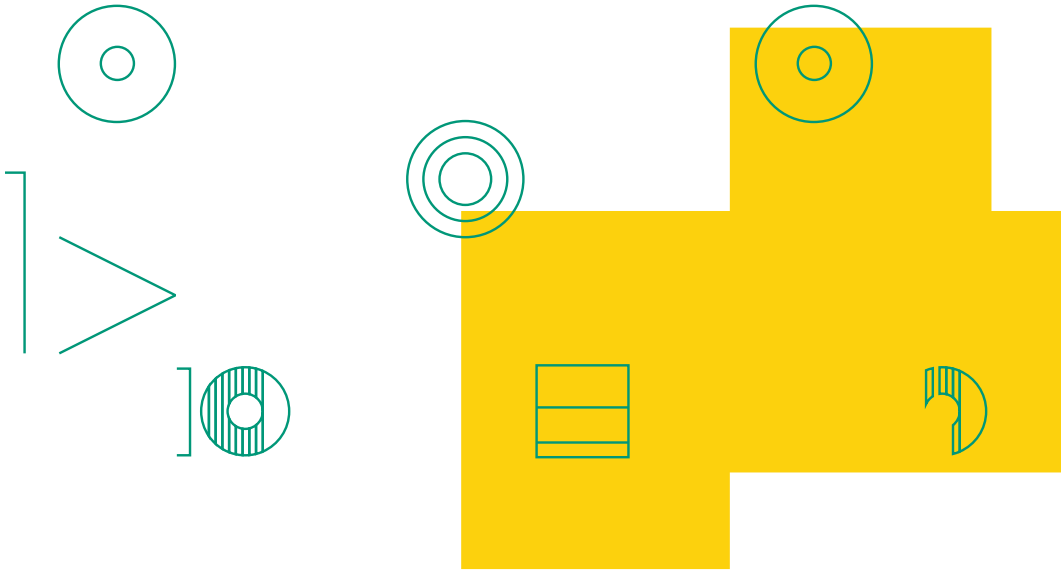
Privacy Protections When Vendors Don't Align

The □nal decision to acquire vendor products may technically be made by the library; however, the political cost of not getting a database or product may simply be too high. When a product is so popular with users, or when a powerful person in your organization (professor, administrator, board member) pushes for a product, your library may need to acquire the product despite your concerns over user privacy.

Even when you can't control the selection of a product you feel doesn't protect user privacy, you can still take short-term actions to protect user privacy:

- Educate users through website notices before they leave the library website to navigate to a vendor resource.
- Use library instruction sessions and library e-resource product promotions as opportunities to educate users about the privacy risks of using vendor products and ways they can protect their personally identi□able information (PII).
- Advocate for adoption of aggregated metrics for internal use, particularly with software that identi□es individual users.
- Do not retain personally identi□able information from vendor usage reports. Use aggregated totals when possible.





There are a couple of ways you can ask a vendor about their privacy practices:

- Tell them speci□cally what you want, such as “Vendor must use [speci□c level of] encryption for data storage and transit”, or
- Ask how they meet a certain privacy criterion, such as “What are the security measures in place to protect user data in storage and in transit?”

Each way has its strengths and weaknesses. Asking if a vendor meets certain criteria can make evaluation quicker, but it might leave out important details about how the vendor meets that criteria. The details from asking how a vendor meets certain criteria, though, might be lacking and might require additional back and forth with the vendor.

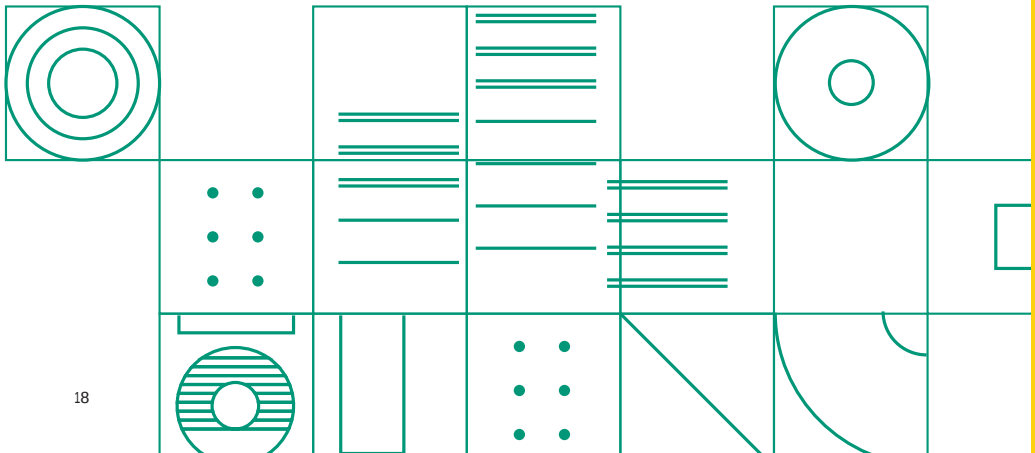
Contracts and Licensing

Contracts and licenses are legally binding documents that state the expectations,

Contract Red Flags

Here are some common contract red flags:

- "Reasonable" and use of vague terms; overall lack of transparency on data privacy and security
- Lack of definitions for terms (such as "data")
- Indemnity/liability clauses that leave the vendor blameless when something goes wrong on their end
- Lack of information regarding what happens to data after termination of the contract
- Lack of information about responses to law enforcement or government data requests
- Vendor claims ownership over library user data
- Vendor reserves the right to resell or disclose user data to other third parties for marketing or other non-essential business purposes
- Vendor reserves the right to monitor users on services or products (including use of web analytics products or other tracking software or methods)
- Using "Aggregated," "Anonymized," or "De-identified" without defining these methods
- Providing a URL to the privacy policy on the vendor website. The policy on the website can change at any time without renegotiation of the signed contract



EXERCISE / SCAVENGER HUNT

If you have access to a vendor contract, read through the contract and compare it with the list of red flags.

What vendor contract(s) did you look at?

What red flags did you find?

What other red flags not listed did you discover?

What else did you find that you didn't understand?

Take these red flags to your vendor or library worker that handles vendor contracts. Express your concerns and ask for clarification.

Pushing for Privacy in Your Organization

If other units, such as information technology services or legal counsel, have a say in your acquisition process, learn their policies and standards around privacy.