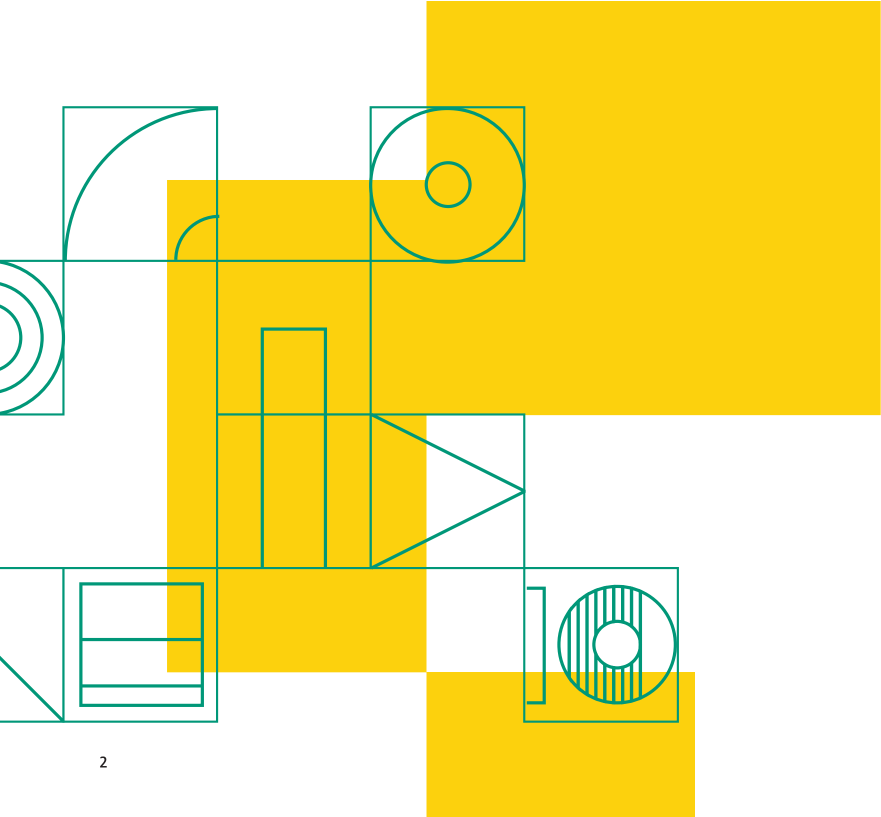
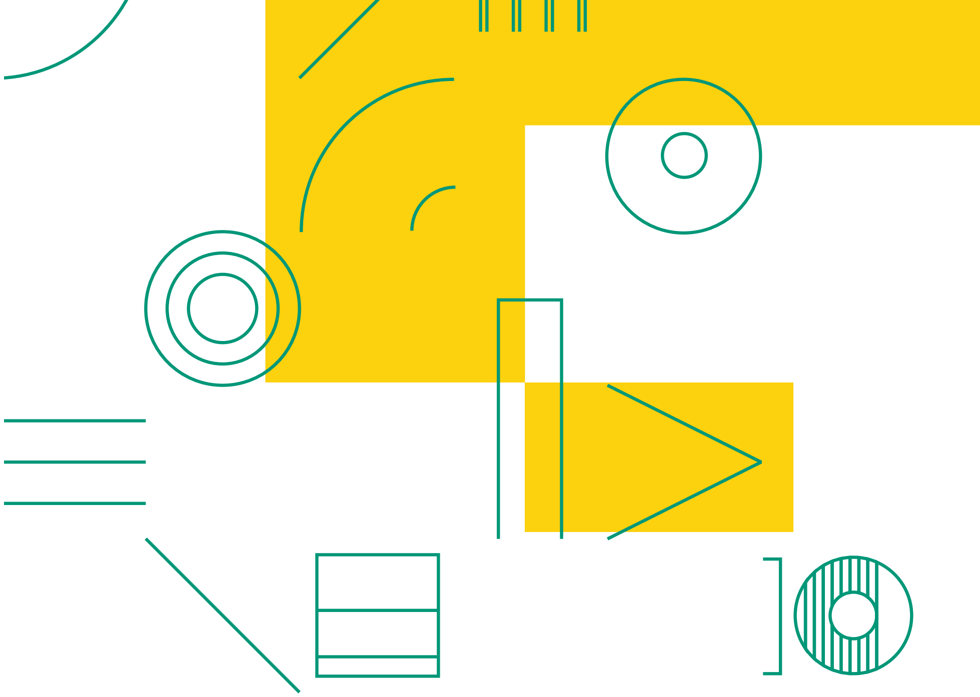
VENDORS AND PRIVACY

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.

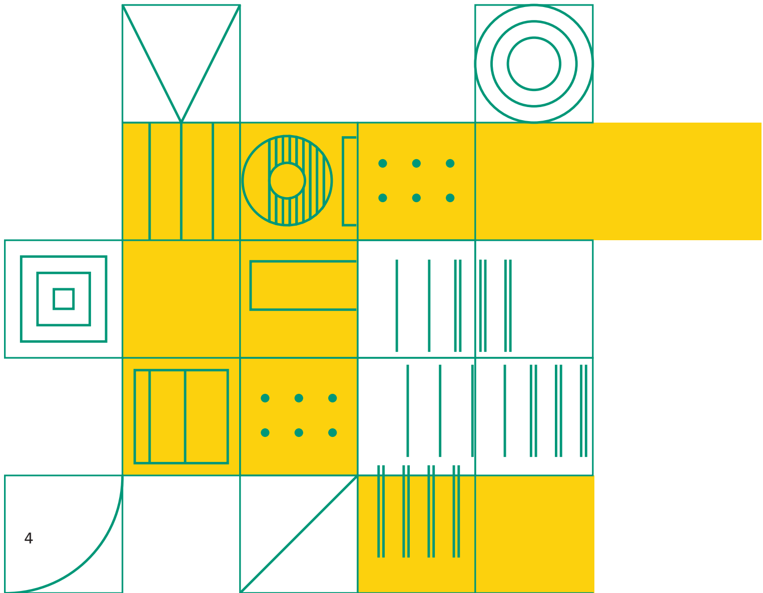




Who Controls the Decision to Buy?

Institutions have a wide range of purchasing processes. Some library workers have sole discretionary power over acquisition of vendor electronic resources or software. In this case, you can choose your standards regarding privacy and refuse to purchase products that don't meet your standards. For library workers with full control over purchasing, this guide can provide ideas of what to look for regarding privacy, and how to see if the vendor or the product meets those standards.

More commonly, a single library worker does not have complete control over purchasing. In some cases, library workers select some software and electronic resources, while other software is selected by a different part of the institution. In addition, libraries may have control of the product selection, but the purchase process may require the product being approved by another department, such as Information Technology Services (ITS), legal, or overall organizational administration or governing body. In that case, the vendor product may be held to those departments' privacy policies and standards, which might not be as extensive as the library's privacy policy.



EXERCISE

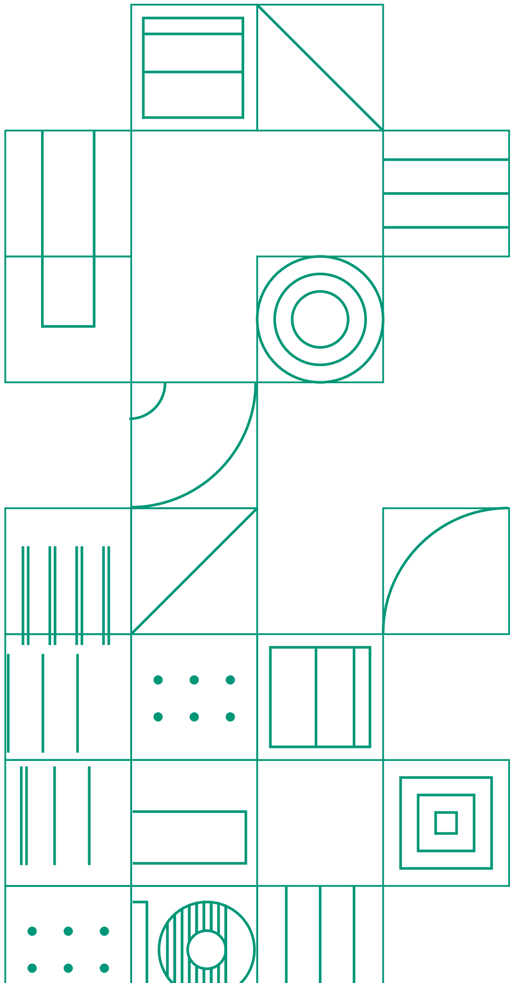
Investigate the vendor selection process at your library by listing the answers below.

1. Write the name of each library staff member involved in the vendor selection process.
2. What is their role in the selection process?
3. Do they consider privacy in evaluating resources?
4. Are there opportunities to discuss with them how privacy should be part of the evaluation?

1. STAFF NAME	**2. ROLE**	**3. Y/N**	**4. Y/N**
Nancy	*Approves Invoices*	*N*	*Y*
Raul	*Oversees RFP Process*	*Y*	*N*

Don't know a person in the process? Wondering how to figure out who you need to convince to become a library privacy ally? Check out the "How to Talk About Privacy" Field Guide!

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.

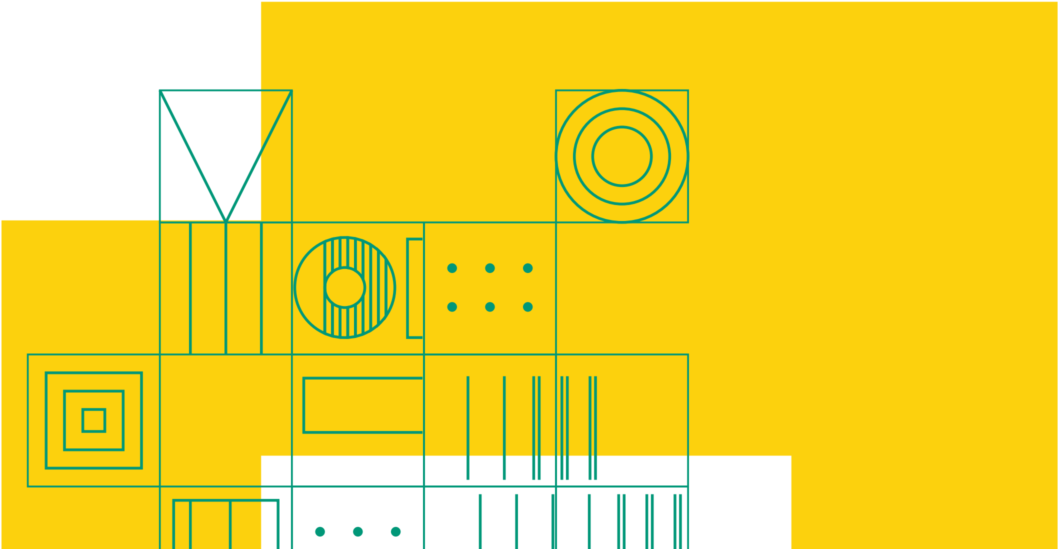


Privacy Protections When Vendors Don’t Align

The final 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 identifiable information (PII).
- Advocate for adoption of aggregated metrics for internal use, particularly with software that identifies individual users.
- Do not retain personally identifiable information from vendor usage reports. Use aggregated totals when possible.



The What, When, and How of Evaluating Vendor Privacy

Selection - Shopping with Privacy in Mind

The first and best place to protect user privacy is during the vendor selection process. Libraries who have sole discretion as to which products to buy have the greatest amount of control in this area. For other libraries, this might not be the case. However, this does not mean that libraries can't have privacy-conscientious products! Refer to the "Who Controls the Decision to Buy?" section in this guide for strategies in selecting privacy-conscientious products when the library is not the primary decision maker in the selection process.

Selecting a vendor product can be overwhelming when there are a variety of choices, while at other times a dearth of choices can make the process extraordinarily underwhelming. In both cases, libraries still need to do their research into each vendor's privacy practices. The research done up front can save you time down the road during the contracting process as well as reduce the chance of surprises around vendor privacy practices.

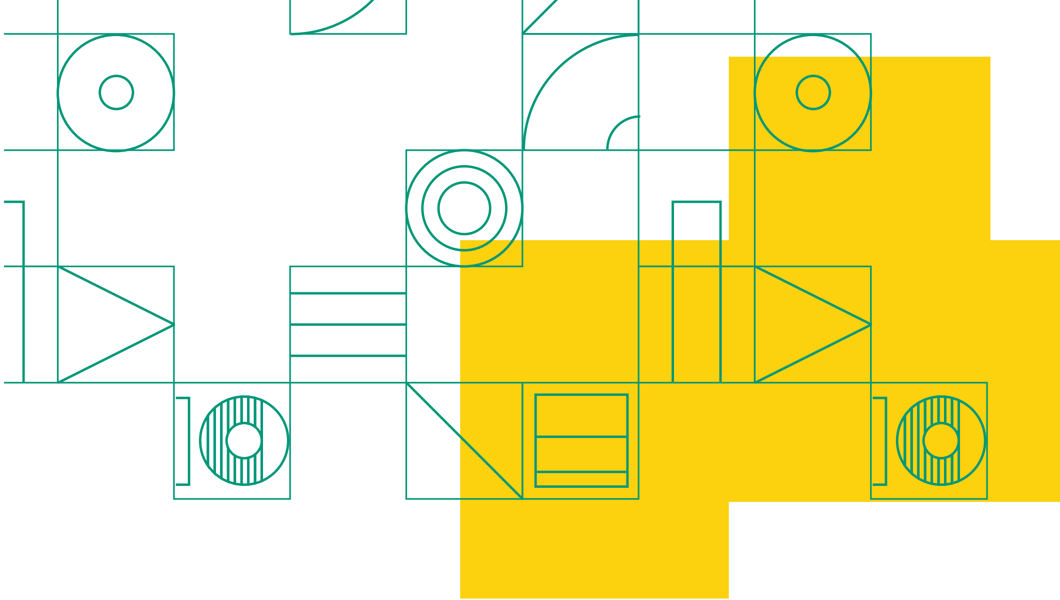
Having a systematic way to evaluate vendor choices can help save time and resources, as well as ensure that each vendor is evaluated with the same set of criteria. Depending on the organization and nature of the proposed purchase, libraries might be able to use a Request For Proposals (RFP) to collect information from vendors for evaluation. RFP templates can be updated to include questions around data privacy and security practices, as well as list privacy requirements that the vendor must meet in order to be considered for selection.

EXERCISE

- How does your library's vendor selection process assess vendor privacy practices?

- How can you incorporate privacy requirements and questions into that process, including in the RFP?

- Use this Annotated RFP Guide (http://bit.ly/annotateRFP) for examples of different approaches.



Evaluation Questions and Standards

Even if your library isn't required to go through the RFP process, you can use any of these questions or standards to ask vendors while you're evaluating products. Here's a short list of what to search for when researching vendor products for selection to get you started:

- Does the vendor have a publicly available privacy policy?
- What user data does the vendor collect, process, and disclose to third parties? What rights do users have to their own data? Is there an opt-out option?
- How does the vendor store user data? Is the storage encrypted? Where is the storage located? Is it hosted by a subcontractor? Is it stored outside of the country? Is it stored in the cloud or on a local server?
- Does the vendor meet specific information security standards, such as ISO/IEC 27001 or PCI-DSS, or use specific information security and privacy frameworks, such as the NIST Cybersecurity Framework and NIST Privacy Framework?
- What fourth parties or subcontractors does the vendor disclose user data with and for what reasons?
- How does the vendor meet applicable federal and state legal regulations regarding data privacy and security?

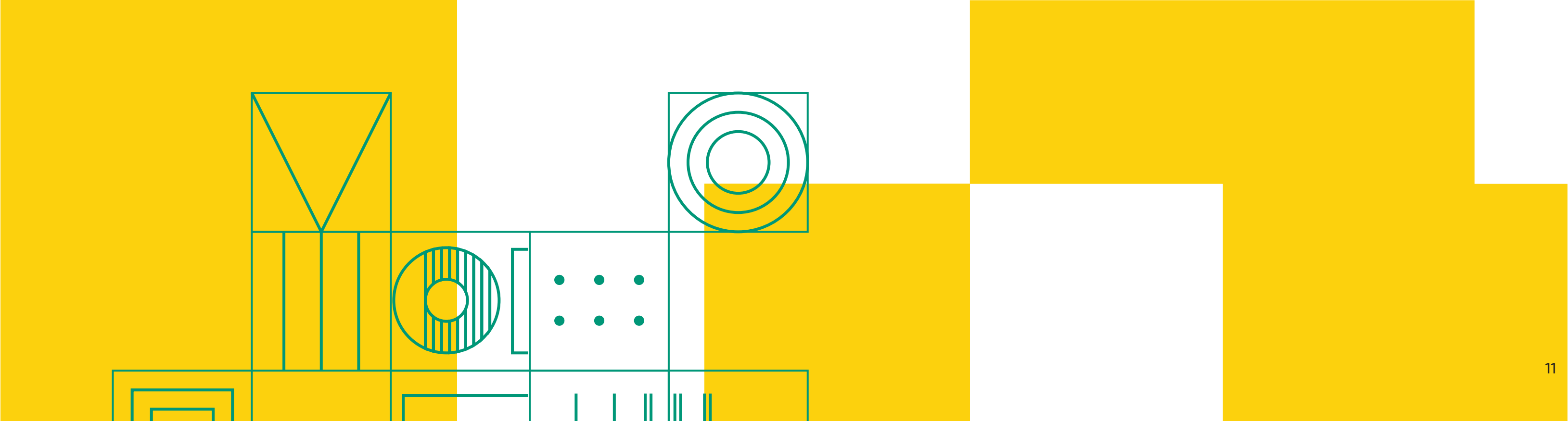
Learn more about these standards:

ISO/IEC 27001
http://bit.ly/privacy27001

PCI-DSS
http://bit.ly/privacypci

NIST CYBERSECURITY FRAMEWORK
http://bit.ly/privacyNIST

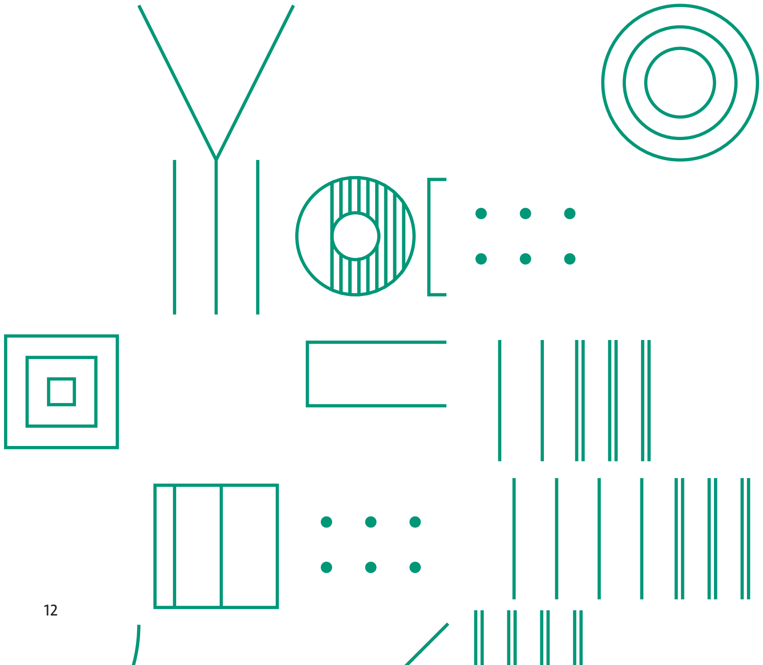
NIST PRIVACY FRAMEWORK
http://bit.ly/NISTframe



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

- Tell them specifically what you want, such as “Vendor must use [specific 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.



EXERCISE

Think of a specific privacy criteria you want included in an RFP. Write two ways to approach the vendor.

- Tell them specifically what you want.

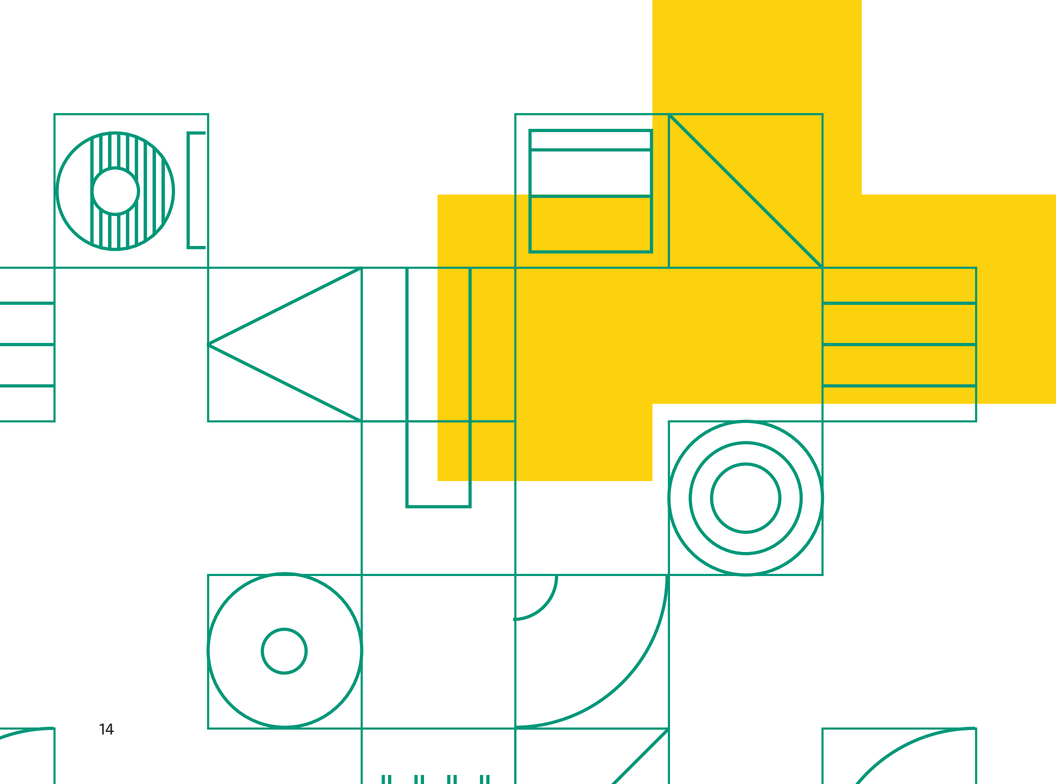
- Ask how they meet the specific criteria.

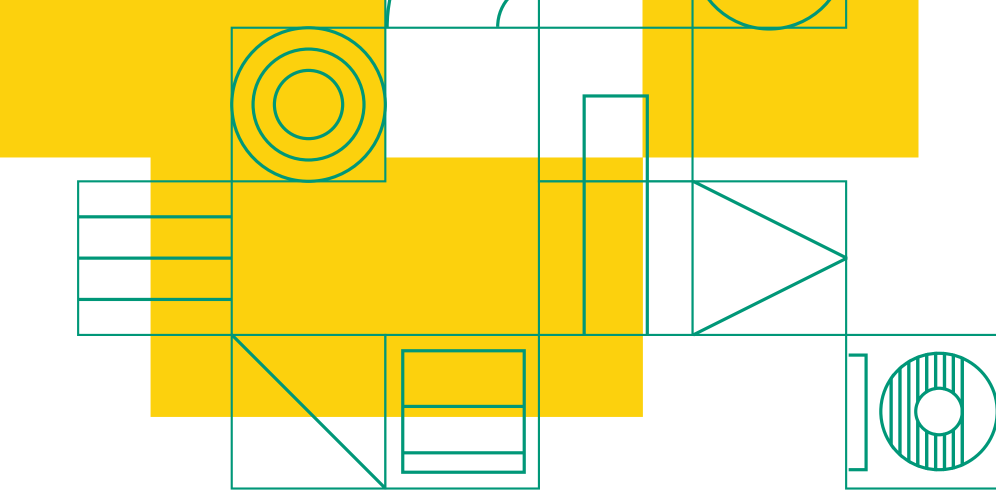
- Which would be the most effective way to ask the vendor, and why?

Contracts and Licensing

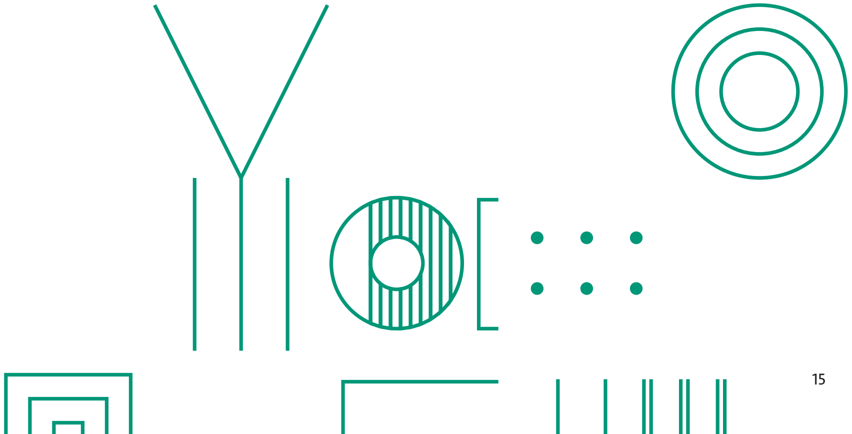
Contracts and licenses are legally binding documents that state the expectations, rights, and responsibilities of all parties involved. They can also give vendors and other third parties rights to collect, process, and disclose user data, compromising user privacy. With some advanced planning and careful reading, you can identify these privacy risks and negotiate with the vendor for more privacy-friendly terms.

Contracts' use of legal language can make them very dense and oblique for the average library worker reading them. Contracts might say that the vendor protects user privacy, but vendor privacy standards may not be the same as your library's privacy standards.





Contract negotiation can be a stressful and complicated process. Identifying which areas you're willing to compromise on as well dealbreakers before the negotiation process can help. Do not be afraid to end negotiations over dealbreakers! There are other vendors who might have better privacy practices. Additionally, a vendor might be pressured to change its contract or its practices if enough libraries refuse to sign or renew contracts because of dealbreakers.



EXERCISE

Here are some examples of language from actual contracts. You can see the variety of approaches to privacy. What possible privacy risks or protections can you find in the examples?

1. "We take privacy very seriously. While we do log information on visits, queries and other site activity, this information is for evaluating the effectiveness and usefulness of [product name] only. All specific visit information is treated confidentially and anonymously, and is never shared with any other party, including the participating distributors. Aggregated data is shared with distributors."

2. "The Parties agree to maintain the confidentiality of any data relating to usage of the Licensed Materials by the Licensee and its Authorised Users. Such data may be provided to third parties in aggregated form only and shall not include any information relating to the identity of individual Authorised Users."

3. "Any and all transfers of personal information will be in compliance with applicable laws and regulations, including, the Health Insurance Portability and Accountability Act ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), the Family Educational Rights and Privacy Act ("FERPA"), and [State] Statutes §817.5681."

4. "Licensor shall be entitled to hold and process the personal data of Participating Institutions and Authorized users as defined in applicable privacy and data protection legislation; make such information available to (i) business partners, sub-contractors and/or suppliers who provide products, or services to Licensor; (ii) our branches; either of whom may be outside the European Economic Area for legal and administrative purposes in order to fulfil its obligations under this Agreement."

ANSWERS

1. Admit they track user behavior. Aggregated data is shared, but not PII. "We take privacy seriously" has no legal meaning.

2. Aggregated data is shared; no PII data is shared.

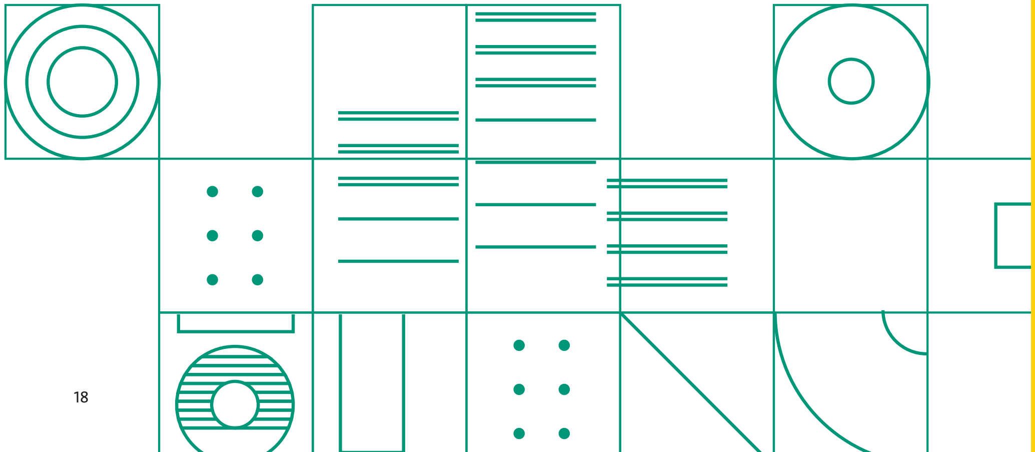
3. Anything not covered by HIPPA (not relevant), FERPA, HITECH and local state laws is fair game to be shared, this could be a lot of data.

4. Personal data is shared with business partners, subcontractors and suppliers in regions where GDPR doesn't apply. "Fulfil its obligations" is not defined, could be broad.

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.

Making the Contracting Process Consistent

One way to make the contracting process more consistent across vendors is a contract addendum. Contract addendums (when reviewed and vetted by legal staff) provide standardized legal language around the level of privacy and security expected of the vendor by the library. Changing or amending the main contract language or including a contract addendum can address the common red flags listed earlier, as well as set responsibilities, rights, and expectations around:

- Compliance with applicable federal, state, and local laws and regulations addressing data privacy
- Compliance with applicable industry standards and frameworks such as ISO, NIST, and PCI
- Legal jurisdiction of the contract; that is, what state or country's laws will apply when interpreting the contract or deciding a dispute
- Vendor privacy and security audits done by either an independent third party or self-administered by the vendor
- User rights to data, including access and deletion
- User rights to opt-out of non-essential data collection by the vendor, as well as the right to opt-out of the disclosure or selling of their data by the vendor to other third parties, at any time
- Abiding by the library's privacy and confidentiality policy when collecting, processing, and disclosing user data and abiding by any laws or regulations applicable to library users' information
- Levels of access to and proper use of user data in the case of integrating with other library systems and applications
- User data retention periods
- Data breach and incident response

EXERCISE

Using the same vendor contract from the red flag exercise, start a list that could lead to a contract addendum draft.

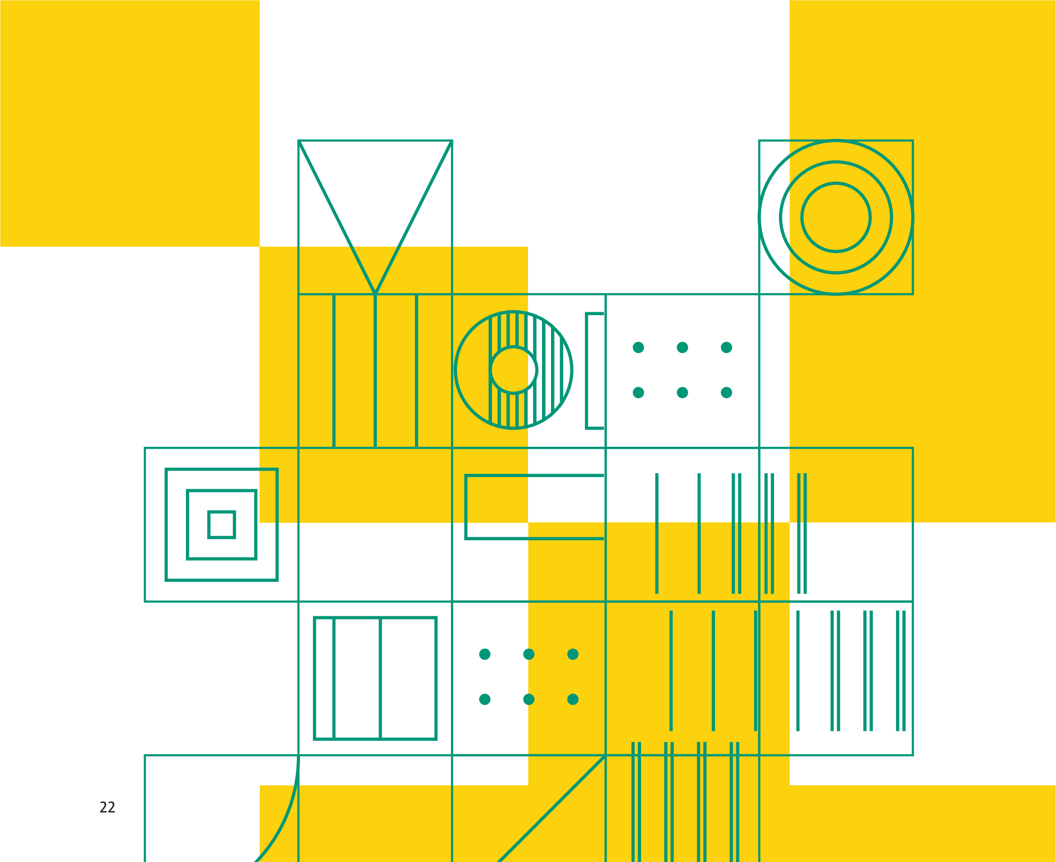
- How can the contract be improved?

- What requirements around privacy do you expect/desire across all vendors?

Start drafting a contract addendum for your library. Examples can be found here http://bit.ly/ContractAdden. Work with your library's governing body and legal counsel to finalize an addendum.

Vendor Audits

Users trust the library to protect and secure their data, including when the library works with vendors or third parties to provide services and resources. How can libraries ensure that vendor data practices don't betray that trust? Libraries can ensure that vendors are following contractual terms and other legal obligations, as well as complying with specific data privacy and security standards and practices, by employing data privacy and security audits. These audits, conducted either by an independent third party or self-reported by the vendor, can identify any potential risks to user privacy, such as unnecessary data collection or disclosure, or potential weaknesses to security practices, such as how the vendor controls access to user data in their organization.



Examples of vendor audits:

- **VENDOR SECURITY ASSESSMENT QUESTIONNAIRE (VSAQ)**
  http://bit.ly/LibraryVSAQ
- **HIGHER EDUCATION COMMUNITY VENDOR ASSESSMENT TOOLKIT (HECVAT)**
  http://bit.ly/LibraryHECVAT

Keep in mind:

- APIs (Application Programming Interface) and any LTI (Learning Tools Interoperability) should be evaluated for privacy risk. If they integrate into course management software and individual students' accounts, then those vendors potentially have access to users' data.
- Apps that allow for access to vendor resources should also be evaluated for privacy risk.
- Review vendor products for any additional "freebie" services or products not covered under existing contracts. For example, a vendor might provide access to another product at no cost in addition to the paid resources or services. A free product collects, stores, and shares data all the same as a paid product, but without any privacy protections provided in the paid product's contract.

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. They might cover only a legal minimum (legal compliance) or they might only be concerned about privacy protections for the data that the institution has to provide for the product. They might not be concerned about data the user can additionally provide, leaving that user data vulnerable to possibly harmful vendor data practices.

If you're part of a larger organization, find out if it has a privacy officer or someone with privacy in their job responsibilities. In academic institutions, these people may be focused on course management software or early warning student monitoring, and library databases and other resources might not be on their privacy radar.

TIP | If you find negotiating on your own stressful, find privacy advocates and allies from your organization to help. For example, the IT department might have strong data privacy and security standards that you can refer to if another department pushes for a privacy-violating vendor resource.

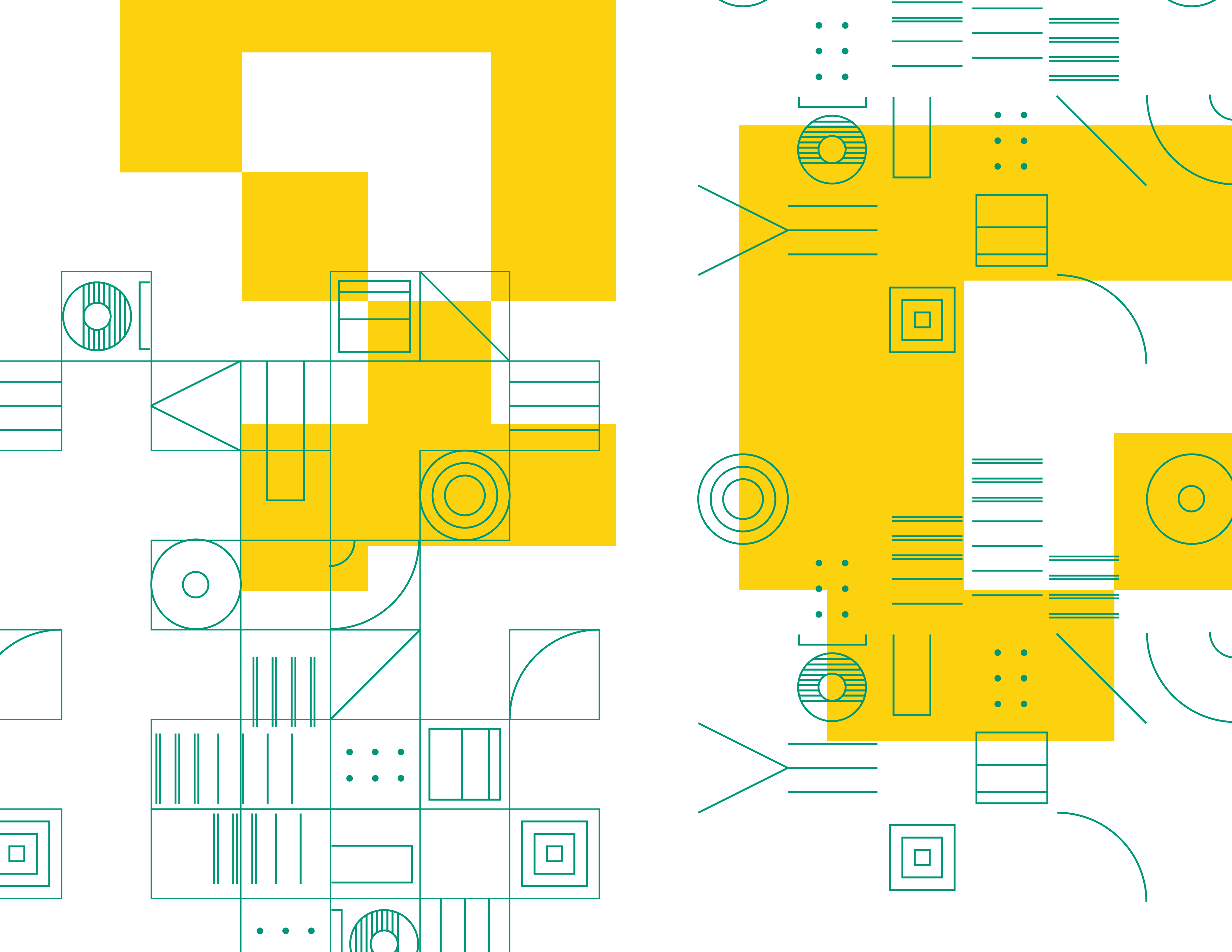
EXERCISE

Pick a vendor product; electronic resource, database, or system.

- What is the minimum amount of information a user must provide to use the basic version of this product?
- What additional information does a vendor require to use all the product features?

Compare the two lists.

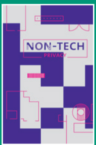
- How much additional user data is collected if the user decides to use the additional functions and services?
- Does the product encourage users to provide personally identifying data for personalized services?



ALA American Library Association

PRIVACY ADVOCACY GUIDES

Privacy is a core value of librarianship, yet it often feels like an overwhelming and onerous undertaking. Use these Privacy Field Guides to start addressing privacy issues at your library. Each guide provides hands-on exercises for libraries. Check out all the available guides at **bit.ly/PrivacyFieldGuides.**



INSTITUTE of Museum and Library SERVICES

This project was made possible in part by the Institute of Museum and Library Services LG-36-19-0073-19.

Designed by
PixelbyInch.com