Licensing Privacy Project

Developing the Vendor Contract and Policy Rubric

LDH Consulting Services
January 2022
Project statement
The Licensing Privacy Project\(^1\) seeks to use the power of library licensing agreements to effect change in third-party platform practices in order to bring them into alignment with library values of privacy, confidentiality, and respect for user control over their own data. It reflects an identified Pathway for Action from the IMLS-supported National Web Privacy Forum.\(^2\) The goal is to develop model license language on user privacy that would support libraries in advocating for user privacy when contracting for services and content. By ensuring that user privacy is contractually protected in licensing agreements, service contracts, etc., libraries would be able to hold platforms accountable for their data practices.

Funding and License Statements
This white paper was developed by LDH Consulting Services as a component of the Licensing Privacy Project led by Lisa Janicke Hinchliffe. This project was made possible in part by The Andrew W. Mellon Foundation.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

Acknowledgements
We would like to thank the following people who graciously donated their time and energy in reviewing and providing feedback on a beta version of the Vendor Contract and Policy Rubric:

- Freeda Brook
- Nora Dethloff
- Scarlet Galvan
- Hannah McKelvey
- Ann Okerson
- Scott W. H. Young
- Katie Zimmerman

\(^1\) [https://publish.illinois.edu/licensingprivacy/](https://publish.illinois.edu/licensingprivacy/)
\(^2\) [https://scholarworks.montana.edu/xmlui/handle/1/15445](https://scholarworks.montana.edu/xmlui/handle/1/15445)
# Contents

Introduction.........................................................................................................................................................1

Negotiating Privacy, Navigating Hurdles............................................................................................................1
  Many Professional Standards, Little Consensus.................................................................................................1
  Changes in Players and Power at the Negotiation Table....................................................................................4
  A Navigation Tool for the Negotiation Process.................................................................................................4

Developing the Vendor Contract and Policy Rubric.............................................................................................4
  Research...........................................................................................................................................................5
  Drafting............................................................................................................................................................5
  Testing and Revision.........................................................................................................................................8
  Rubric Limitations............................................................................................................................................9

Using the Rubric – A Starting Point....................................................................................................................9

Appendix A – Resources.....................................................................................................................................11

Appendix B – Glossary.......................................................................................................................................12

Appendix C – Example Contract Language.....................................................................................................15

Appendix D – Rubric (Static Version)................................................................................................................20
Introduction
The shift from physical ownership to licensing materials has shifted power dynamics between libraries, their institutions, and vendors. One part of this shift centers around the amount of control libraries have around patron privacy risks. Academic libraries are more reliant on third parties involved in the licensing process than they had been in the past when the majority of the library’s resources were physically owned by the library. This in turn places negotiations around vendor licenses front and center in determining what the vendor has the right to do, including the management of patron data collected from their platforms. Because the license is a legal document, the library has legal recourse if the vendor does not abide by the responsibilities or terms stated in the contract around patron data privacy.

Reviewing and negotiating contracts are not simple endeavors. Contract language can be dense, obfuscated, or vague for those who are not trained or are inexperienced in reviewing contracts. Experienced reviewers are better equipped in navigating contract language, but might struggle to draft language to fill in the gaps where a contract lacks desired language around data privacy protections. Even when the reviewer identifies potential privacy issues and how these issues can be mitigated in the contract, the reviewer has to find a way to persuasively communicate these changes to others involved in the negotiation. Reviewing and negotiating for patron data privacy in the context of platform contracts only adds to the complexity of these endeavors.

This white paper will explore specific issues that academic libraries face while reviewing and negotiating content platform contracts, such as conflicting professional privacy standards and managing intra-institutional relationships with those involved in the negotiation process. The paper will then discuss the creation and development of the Vendor Contract and Privacy Rubric, a tool developed by the Licensing Privacy Project to aid academic libraries in the reviewing and negotiation processes, as well as how this tool can be used to address the specific data privacy issues.

Negotiating Privacy, Navigating Hurdles
Taking on the task of reviewing contracts for potential data privacy and security issues means navigating through not only the contract language but also through various hurdles in the process itself. Sometimes these hurdles are not apparent at first, only to make themselves known after the fact when the process or negotiation breaks down. Contract language can be a hurdle when the reviewer or negotiator does not identify gaps in the existing contract that could lead to privacy risks and harm. The Licensing Privacy Project aims to provide model contract language to mitigate the privacy risks that come from absent or vague contract language. Nevertheless, model language is only one tool in a process; a multi-pronged approach is required to mitigate data privacy risks. Academic libraries face hurdles that model language does not fully address, in particular the current lack of consensus on data privacy standards in the profession and the evolving negotiation processes in higher education.

Many Professional Standards, Little Consensus
Academic libraries are not wont for standards and resources when it comes to privacy and security. The library profession contains a plethora of codes, standards, and best practices around library patron privacy and confidentiality. The American Library Association addresses the profession’s responsibilities to protect patron privacy through professional codes such as the Code of Ethics and the Library Bill of Rights. ALA resources such as the Privacy Toolkit and Library Privacy Guidelines and Checklists, as well as privacy resource clearinghouses and blogs featured on the Choose Privacy Every Day website, provide
library practitioners guidance on privacy practices in their libraries. The International Federation of Library Associations and Institutions (IFLA) also addresses professional responsibilities to protect privacy through the IFLA Statement on Privacy in the Library Environment. Academic libraries in the US can also turn to the Association of Research Libraries and regional or state library associations and consortia for additional guidance on patron privacy practices. Publications, presentations, and assessment templates provide case studies on implementing privacy practices at academic libraries, providing yet more guidance on best practices around patron privacy.

Beyond professional library organizations, academic libraries can also refer to resources geared toward higher education for data privacy and security standards and practices. EDUCAUSE’s Higher Education Community Vendor Assessment Toolkit (HECVAT) is one example of a widely used suite of tools and resources to assess vendor data privacy and security practices in US higher educational institutions. Other data privacy and security standards and practices come from collaborative efforts among higher education stakeholders, libraries, publishers, and vendors, as is such the case with the Educopia Institute’s Values and Principles Framework and Assessment Checklist and NISO’s Privacy Principles.

On the surface, the plethora of codes, standards, and resources available seem to provide academic libraries ample guidance in identifying and addressing data privacy risks in vendor contracts and policies. Digging deeper into these resources, however, reveals a hidden hurdle – a lack of consensus around acceptable privacy standards and practices. To some, this lack of consensus is expected when comparing library and general higher education resources around data privacy, much like differences in the privacy policies of the academic library and the educational institution of which the library is a part. Each entity has to comply with not only a shared set of regulations and standards but also have regulations and standards unique to that entity (such as the academic library when state regulations around library privacy pertain to academic libraries). While some variance between standards and practices between different industries should be expected, academic libraries face the complication of conflicting and contrasting levels of acceptable privacy within the foundational codes, standards, and other resources of the profession itself.

Sometimes the contrast occurs between professional organizations. Comparing the IFLA Statement on Privacy in the Library Environment to ALA standards and subsequent interpretations of those standards reveal a difference in the level of acceptable surveillance of patrons by third parties (such as content platform vendors). The Code of Ethics and Library Bill of Rights both charge libraries to protect patron privacy, including patron data, but ALA’s “Privacy: An Interpretation of the Library Bill of Rights” does not explicitly address surveillance of patron use of vendor products and services beyond a cursory mention near the end:

“The use of new technologies in libraries that rely on the collection, use, sharing, monitoring and/or tracking of user data may come into direct conflict with the Library Bill of Rights and librarians’ ethical responsibilities. Libraries should consider privacy in the design and delivery of all programs and services, paying careful attention to their own policies and procedures and that of any vendors with whom they work.”

IFLA’s stance on surveillance in any form is made explicit in the *Statement on Privacy in the Library Environment*:

“Library and information services should reject electronic surveillance and any type of illegitimate monitoring or collection of users’ personal data or information behaviour that would compromise their privacy and affect their rights to seek, receive and impart information. They should take measures to limit collection of personal information about their users and the services that they use.”

The IFLA Statement recognizes that libraries have limited influence over vendors, but still directs libraries to negotiate with vendors to reduce or eliminate privacy-invasive practices. IFLA also clearly states that libraries should not do business with vendors who collect excessive amounts of patron data and should limit use of technologies in libraries that compromise patron privacy. In comparison to IFLA, ALA’s standards are vague and leave room for privacy-invasive practices. For example, when the ALA Interpretation document addresses biometric technologies, it is only to point out that these technologies are “inconsistent with the mission of facilitating access to library resources free from any unreasonable intrusion or surveillance.” The ambiguity in this statement does not direct libraries to any particular action or give guidance. Even though the IFLA Statement does not explicitly call out biometric technologies, it is still a surveillance technology that the Statement calls for libraries to reject outright.

Another factor in the lack of consensus around library privacy standards is that these standards are drafted for different audiences by different organizations with different priorities. For example, content platform vendors have the option to use ALA standards and resources to inform data privacy practices, but the primary audiences for ALA resources are libraries. There is currently no incentive for library vendors to adhere to the ethical codes of the profession nor does the profession provide concrete incentives to vendors for compliance. Attempts to bridge the gap between different audiences and organizations have been mostly lackluster at best, with a prominent example being the *NISO Consensus Principles on Users’ Digital Privacy in Library, Publisher, and Software-Provider Systems* (NISO Privacy Principles). The *NISO Privacy Principles* document was created in 2015 by a process involving library workers, professional organizations, and vendors as an attempt to create a shared standard for vendors and libraries. However, adoption of these principles by libraries has been inconsistent at best, and no systematic review of vendor adoption has been conducted as of 2021. In addition, the *NISO Privacy Principles* have been the subject of scrutiny by library workers, noting areas where stakeholder incentives to continue privacy-invasive practices as well as prioritizing these practices weakens the protections to patron privacy. The lack of consistent adoption of standards by libraries and vendors,

---

5 ALA, “Privacy.”
coupled with the lack of general consensus around privacy ethics and practices in library codes and standards, make any process around data privacy assessment and review a tedious exercise fraught with potential hidden privacy risks for patrons.

**Changes in Players and Power at the Negotiation Table**

Academic libraries also face the hurdles that come with the changes in the negotiation process due to the shift from physical ownership to licensing of library materials. The addition or increased presence of organizational stakeholders – such as purchasing offices, consortia staff, and campus administration – can lead to a loss of control by the individual library over privacy language and practices. For example, a content platform vendor who builds direct relationships with influential faculty and staff in the negotiation process could lead to these parties being less likely to push back on privacy-invasive contract language during negotiations. These parties might be influenced by the level of trust developed in the direct relationship, or they might have priorities that conflict with preserving privacy, such as learning analytics initiatives.

Sometimes the hurdles compound existing organizational issues, particularly around intra-organizational relationships and communication. An example of organizational issues compounding existing hurdles is the inconsistent messaging around privacy if all members of the institutional side of the negotiation table – including the academic library – are not in agreement as to the level of privacy that should be included in the contract. Intra-institutional relationships between offices and departments can play into this confusion if these relationships are weak or non-existent.

**A Navigation Tool for the Negotiation Process**

It is the accumulation of hurdles that leads to the need to develop a tool that can navigate these challenges in an efficient manner. Nevertheless, there might be additional hurdles in the negotiation process that could also impede the library’s ability to review and negotiate for data privacy during the contract negotiation process. Any tool built to navigate the first two hurdles should also be flexible enough to aid libraries in navigating additional hurdles specific to their institution. The next section describes the development of such a tool, the Vendor Contract and Policy Rubric, with the goal to provide a streamlined and versatile tool for libraries to add to their collections of strategies and approaches used for content platform contract negotiations.

**Developing the Vendor Contract and Policy Rubric**

The Rubric development process consisted of research, drafting, testing, and revision based on test feedback. The appendices contain a static version of the Rubric and supplemental material published in October 2021. While this section will not be exhaustive in discussing every factor in the development process, it aims to provide a general sense as to what went into developing the Rubric.

**Research**

As mentioned earlier, there is no shortage of privacy standards and resources for academic libraries to consult in evaluating vendor privacy practices. The full list of resources consulted for the development of the Rubric can be found in the Appendices. These resources were sorted into two categories:

- **Standards and Codes** – These resources provide the framework or core elements around the level and types of privacy protections, as well as indicate what level of priority these protections
should take in policy and practice. ALA’s Code of Ethics and IFLA’s Statement on Privacy in the Library Environment are examples of resources in this category.

- Assessments and Guidelines – These resources provide a more granular description of the level and types of privacy protections that should be incorporated into policy and practice. The resources can also assess existing policies and practices to their adherence to a particular privacy practice or standard. The Library Freedom Project’s Vendor Privacy Scorecard and EDUCAUSE’s HECVAT are examples of resources in this category.

Each resource was assessed on similar but separate sets of elements based on which category the resource belonged to:

**Standards and Codes**

- Target Industry/Audience
- General Summary
- Data Privacy Topics
- Data Security Topics
- Other Relevant Observations

**Assessments and Guidelines**

- Target Audience
- Scope of Resource
- Specific Topics, such as
  - Contracts
  - Separation/end of business relationship
  - Disclosure to other third parties
  - Data ownership
  - Incident response
  - Data processing
  - Data security
- References to Standards and Codes
- Scoring Mechanism and Completion of Assessment By...
- Other Relevant Observations

The analysis of each category highlighted the contrasts between resources as well as some broad consensus around certain topics, such as limiting the disclosure of personal data to third parties. The level of limiting disclosure varied between resources; however, a minimum level could be derived from the review. This pattern of loose consensus among resources on certain privacy topics led to the development of the privacy levels as well as the privacy domains described in the next section.

**Drafting**

The main two content areas of the Rubric derived from the research stage are the privacy levels and the privacy domains.

**Privacy Levels**

While it is true that librarianship has a strong privacy focus, this does not consistently manifest itself in the standards and practices even within the same professional organization. The analysis from a core set of resources, however, hinted that a loose consensus of minimum levels of privacy could be derived to assess the level of privacy protections in specific data privacy domains. This led to the development of the concept of Minimum Viable Privacy (MVP). This concept was adapted from the Minimum Viable Product concept from product management, denoting a version of a product containing the barest level
of functionality to be used by end users. The product is not optimized, nor does it contain functionality that would be considered core for many end users, but the product’s basest functions allow for basic use. Minimum Viable Privacy operates in a similar fashion in that the type of privacy protections afforded by this set of standards and practices are not optimal nor provide the greatest amount of protection possible, but instead provide a baseline where there are some privacy protections against egregious privacy invasive practices.

The consensus of library data privacy standards and practices that make up the MVP come from the following resources, selected based on widespread awareness, availability, and/or adoption:

- ALA Code of Ethics
- ALA Library Bill of Rights
- ALA Library Privacy Guidelines and Checklists (Priority 1) for Vendors
- IFLA Statement on Privacy in the Library Environment
- NISO Privacy Principles
- Privacy: An Interpretation of the Library Bill of Rights (ALA)

Two additional levels were created for the rubric, Exceeds MVP and Does Not Exceed MVP. The Exceeds level incorporates stronger privacy protections from the core resources as well as drawing from other resources from the analysis. The Does Not Meet MVP indicates not only practices that do not meet MVP but also address contract language or data practices that indicate privacy-invasive practices as well as a lack of language around the vendor’s practices in a specific privacy domain.

Meeting or exceeding MVP in a specific privacy domain does not necessarily mean that the vendor is adequately protecting patron privacy. Many of the resources analyzed do not reflect the full spectrum of privacy risks patrons face in their use of the library, particularly patrons in minoritized groups. Professional standards also often do not reflect the most current and comprehensive set of data privacy practices and risks. Assessment around the evolving risk in each privacy domain is required to determine the potential harm if a particular privacy risk is realized.

Privacy Domains

The resources covered a wide range of data privacy and security topics as highlighted in the research stage. While the challenge of conceptualizing privacy levels was one of consensus, determining which aspects – or domains – of data privacy and security to evaluate in the Rubric was a challenge of assessing risk.

Patron data in content platform vendor systems are subject to a set of privacy risks at every stage of the data lifecycle, from collection and processing to disclosure and retention. In addition to the privacy risks in the patron data lifecycle, privacy regulations such as GDPR and frameworks such as the OECD Privacy Principles place user data rights and user control over data collection, processing, disclosure, and retention front and center for businesses and organizations to consider. Certain library patron populations, particularly patrons in minoritized groups, face a higher risk of privacy violations and harms through the data management practices of third parties, in part due to over surveillance and systems that replicate and reinforce systematic bias and oppression.

Logistically, the Rubric needs to aid evaluators in identifying major privacy risks that can have the greatest impact on patrons without losing focus on the finer details of risk assessment in contracts and
policy. The creation of the eight privacy domains in the rubric involved reviewing the privacy frameworks and regulations mentioned above combined with the lens of the data lifecycle and identification of potential harms to patrons if certain privacy risks are realized.

<table>
<thead>
<tr>
<th>Privacy Domain</th>
<th>Questions for Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Collection</td>
<td>What data does the vendor collect, how and where do they collect data, and what is the rationale for collecting it?</td>
</tr>
<tr>
<td>User Data Rights</td>
<td>What controls do users have over the vendor’s ability to collect, retain, use, and share user data?</td>
</tr>
<tr>
<td>Data Disclosure</td>
<td>What data does the vendor share and with which parties? Why is the data shared, and how is data sharing controlled or determined?</td>
</tr>
<tr>
<td>Data Processing</td>
<td>What data does the vendor use, for what purpose, and how is data use controlled or determined?</td>
</tr>
<tr>
<td>Vendor Privacy Policy</td>
<td>What public privacy statements are available on the vendor’s service or website? Are any internal vendor privacy policies provided to the library?</td>
</tr>
<tr>
<td>Data Ownership</td>
<td>Who owns the data in the vendor service or product and what rights come with data ownership in specific business scenarios?</td>
</tr>
<tr>
<td>User Surveillance</td>
<td>What tracking or logging mechanisms does the vendor use to collect user data, and what level of control do users have over vendor tracking and logging behavior while using the service?</td>
</tr>
<tr>
<td>Data Security and Accountability</td>
<td>How does the vendor protect data in transit and in storage from unauthorized access or use? How does the vendor prevent and respond to data breaches or leaks? What checks are in place to ensure compliance to security and privacy policies and standards?</td>
</tr>
</tbody>
</table>

Table 1. Rubric privacy domains and questions for each domain

Supplemental Resources
While developing the Rubric it became clear that the nature of contract language and evaluating contracts based on certain data privacy concepts could be barriers for evaluators who are either not trained to work with contracts or not knowledgeable about data privacy terms and concepts. Vendor contracts might use the same word or phrasing but with different meanings. Privacy regulations have their own definitions for data privacy terms and concepts which further complicates the review process. Terms may have one meaning in everyday use but a constrained meaning in the context of regulations or a contract. On a higher level, contract and policy language can be obtuse, dense, and vague, making evaluation more difficult for those not accustomed to reading legal documents.

To assist evaluators in using the Rubric, two additional resources were created: (1) a glossary of commonly used data privacy and security terms and (2) a collection of example contract phrases for each level of privacy for every domain. The contract examples come from publicly available vendor
contracts, with redactions to remove identifiable information about an individual institution when needed.

In addition to the glossary and example contract language collection, a worksheet was developed for evaluators to record notes, questions, and other observations for each privacy domain being evaluated.

Testing and Revision

The draft Rubric was sent out to seven library workers from various academic libraries and organizations who are involved in electronic resource management, including vendor selection and contract negotiations. Each reviewer was asked to review the Rubric and the supplemental materials based on what would be most useful in their work with vendors regarding data privacy in the licensing process. Reviewers were also invited to work through a vendor contract with the draft Rubric.

Feedback from reviewers were overall positive about the draft. All reviewers noted that the Rubric would be useful in their contract review process, and with additional revisions, would help evaluate specific data privacy and security concerns. Nevertheless, two themes emerged around reviewer concerns about the Rubric that could potentially limit adoption or use of the Rubric.

The first concern was the formatting of the Rubric document. The draft Rubric was a static PDF file that contained both the Rubric and all supplemental materials. Reviewers were concerned about the usability of a static file for a process that involves different stakeholders both within and outside the academic library. The large number of pages in the file meant reviewers had to frequently scroll the electronic file or shuffle through numerous papers in the printed version. The format of the file also led to information overload for several reviewers who navigated between the Rubric and the supplemental materials in their test with a vendor contract. The Rubric in its static PDF form was laborious to navigate and itself was a potential barrier for use.

The second concern pertained to the lack of calculating a final score for the contract using the Rubric. Several reviewers also requested a checklist version of the Rubric criteria. Both the final score and checklist requests centered around the desire to have one main score or take-away from the Rubric for ease of comparing the score with other evaluated contracts. A final score or tally might also quickly convey how strong or weak the contract is around data privacy.

The above feedback led to several fundamental changes to the Rubric and supplemental materials, though the changes were limited to what can be done with the available resources and scope of the project. While reviewers overwhelmingly preferred an interactive web format for the Rubric, resource and scope limitations prevented the project team from moving forward with the suggestion. Instead, the Rubric was shifted from a static PDF file to a combination of web pages and interactive PDF forms. The glossary and example contract language were moved to the Licensing Privacy Project website to address the concern about navigating between the Rubric, the contract, and the supplemental materials. The Rubric and the worksheet were combined to give each privacy domain its own page where evaluators can both evaluate the contract based on the criteria for each privacy level in that domain and make notes about specific risks or questions that come up during the evaluation. The interactive PDF allowed for evaluators to save notes within the file and to share the file with others in the negotiation process. The interactive PDF also automatically generates a list of criteria under the “Does Not Meet MVP” for evaluators to review and share as appropriate. Additional changes to the
Rubric included clarification of privacy level criteria, additional instructions and tips for evaluators, and the addition of check box formatting for each privacy domain page.

The last change – addition of checkbox formatting – did not include a total score or final assessment measure for the rubric. Unfortunately, the complex reality of vendor privacy practices precludes any attempt to create one number or grade. Vendor contracts and policies tend not to neatly fit into one level, but instead have language or practices that fall into two or all three levels. Data privacy practices can vary widely within a given business as well. A vendor might be strong in one data privacy domain and weak in another and a cumulative score could obscure this reality in ways detrimental to the goal of increasing library patron privacy. While there is no final score, a library must take considerable care in negotiations with a vendor that has a significant amount of contract language or practices that fall in the “Does Not Meet Minimum Viable Privacy” level.

Rubric Limitations
Like any assessment tool, the Rubric has limitations and use considerations. Again, a vendor meeting or exceeding MVP in a specific privacy domain does not necessarily mean that the vendor is adequately protecting patron privacy. This is especially true in the data collection and user surveillance domains, where the impact of a privacy breach can have substantial impact on minoritized patrons.

The Rubric is also not meant to review a vendor’s compliance to specific legal standards, nor can the Rubric take the place of an information security audit of the vendor. These reviews are better suited to be conducted by legal counsel and IT staff, respectively, using assessment and evaluation tools developed specifically for those purposes.

Another consideration is that the Rubric is a set document in a rapidly changing landscape around data privacy. The Rubric takes a high-level overview approach to avoid quick obsolescence, but changes around data privacy and technology might affect the evaluation of certain privacy risks in specific privacy domains, particularly in the User Surveillance privacy domain.

The last consideration pertains to labor. During the development and testing stages, both project members and reviewers struggled with the question around who ultimately would evaluate the contract. Adding the Rubric to an already overburdened library worker’s responsibilities are far from ideal. Giving the Rubric to the vendor would lift some of that burden, but could then introduce a self-reporting bias if the vendor self-conducts the assessment, much like when vendors self-conduct security audits. Absent considerable changes in how vendors write contracts and privacy policies, libraries and institutions will most likely carry the additional labor burden.

Using the Rubric – A Starting Point
The Rubric is foremost a tool that is meant to be flexible to meet several needs of academic libraries. Development of the Rubric centered around three potential needs and use cases for academic libraries:

- **Evaluate** – Consolidate professional resources and standards around privacy for ease of evaluating vendor contracts against a privacy baseline
- **Communicate** – Streamline negotiation communications within the library and between the library and others involved in the process
• **Educate** – Use the Rubric to educate others about better privacy protections within the library and within the institution through application of privacy standards at or above the baseline in vendor selection and contract negotiations

The Rubric can be used for any of the use case listed above; however, academic libraries might also consider using the rubric to meet other needs that might be specific to their institution or organization, such as:

• Training library workers and other institutional stakeholders involved in vendor contract negotiations about library privacy standards and criteria.
• Creating or revising contract addendums based on Rubric criteria.
• Revising, expanding, or further consolidating the Rubric criteria to meet specific privacy needs or concerns with content platform vendors.

In addition, the use of the Rubric can span across different academic libraries. In the past, academic libraries and organizations have created contract clearinghouses such as the California Digital Library’s list of redacted license agreements. Academic libraries could additionally create a clearinghouse of completed (and redacted if necessary) rubrics for contracts from content platform vendors.
Appendix A – Resources

Rubric Research Resources

ALA. Library Bill of Rights. https://www.ala.org/advocacy/intfreedom/librarybill


San Jose Public Library. (2018). Vendor Security Analysis. https://drive.google.com/drive/folders/1jdPwQeC5RAUhBoWLAhylYxWHa0pTdVObc

Appendix B – Glossary

Aggregation

A method of de-identification that reduces the granularity of personal data through grouping data into categories or ranges (such as using age ranges to report on user birthdate or age data). Aggregation carries some risk of re-identifying an individual if there are outliers in the data set, if the data set size is small overall, or if categories or ranges are granular enough to identify an individual in the data set.

Anonymization

The process of transforming data that completely breaks the connection between the data and the individual behind the data. Research shows that true anonymization is near impossible, with most anonymization methods retaining a risk of re-identification of individuals in the dataset.7

Behavioral tracking

The practice of surveilling users’ actions over a period of time.

Business purpose

The organizational or operational rationale for a particular process.

Consent

The act of giving or denying permission for the use or disclosure of an individual’s data. Explicit consent requires an affirmative action from the individual, while implicit consent implies consent, such as continued use of a service or website.

Cookies

A small data file sent from the website and stored on the user’s computer or the user’s browser. Web cookies can be used to manage user authorization and session management, as well as track users through web analytic software and other tracking software. Some cookies last until a web session ends (“session” cookies) while other cookies (“persistent” cookies) can remain on the user’s computer after the end of a session. A website can have web cookies from the site itself (“first-party” cookies) as well as cookies from external sites (“third-party” cookies).

Data breach/leak

The unauthorized access of personal data by an individual, organization, or system process. A data breach is an intentional act of gaining unauthorized access, such as an attacker gaining access to personal data for the purpose of identity theft, while a data leak is unintentional, such as an employee losing a laptop or mobile device containing personal data.

Data brokers

Entities that sell personal data collected from private and public data sets.

Data lifecycle
The flow of data from collection to deletion, including processing, disclosure, and retention.

Data minimization
The practice of only collecting and retaining personal data that is necessary to fulfil the purpose for which it is needed.

De-identification
The process of transforming personal data to remove identifiable aspects of the data. This includes a variety of methods, including aggregation, stripping or truncating personal data, or removal or pseudonymization of personal data. De-identified data carries a risk of re-identification, meaning that an individual person can be identified from the dataset by reattaching parts of the dataset back to the individual.

Digital surveillance
The act of monitoring and capturing a person’s activities through various technologies, including web analytics, cookies, trackers, and other data observation and capture techniques.

Encryption
The act of encoding plain data into an unreadable format through use of algorithms or other cryptographical methods. Encrypted data can only be read by someone who can decrypt the data through a decryption key.

Incident response
The process of responding to and managing a data breach or leak. This can include:

- Identification and detection of a breach or leak
- Containing and eliminating the cause of the breach or leak
- Communications with affected parties

Non-personal data
Data that cannot be linked to or associated with an identifiable individual. In some data privacy regulations, this can include data that has gone through rigorous de-identification.

Opt in/out
Opt in is a choice made by a user involving active affirmation, such as checking a box or toggle to turn on specific data sharing or collection settings.

Opt out is a choice made by a user through inaction unless the user makes an action to choose otherwise. An example is a product collecting user data until the user unchecks the box that controls the data collection setting.
Personal data

Data relating to an identifiable individual. This includes single points of data that can identify a person (direct identifier); data that, when combined, can identify a person (indirect identifiers); and data about a person’s behaviors (behavioral data).

Direct identifiers can include:

- Name
- Email or physical address
- Government or organization issued identification numbers
- Account username and password
- Biometric information
- IP address
- Device information (operating system, browser, device unique ID, etc.)

Indirect identifiers can include:

- Age or date of birth
- Race/ethnicity
- Gender identity
- Education level
- Major or minor field of study
- Disability status
- Veteran status
- Geographical information, such as regions or zip code

Behavioral data can include:

- Search history
- Electronic content access histories
- Circulation histories
- Website activity
- Geolocation history

Personally identifiable information (PII)

Information that can identify an individual person or link to an individual person’s identity. See also: Personal data.

Web analytics

The collection and analysis of website data. Web analytic applications track and capture data from a variety of sources, including user data. Depending on the application, user data can range from search term results, page hits, and landing/exit pages to user demographic data, behavioral data, and even data of users visiting sites outside of the original website.
### Data Collection Example Language

<table>
<thead>
<tr>
<th>Exceeds Minimum Viable Privacy</th>
<th>Meets Minimum Viable Privacy</th>
<th>Does Not Meet Minimum Viable Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Use of the service does not require the entering or capturing of personally identifiable user information.</td>
<td>We may collect anonymized information related to your use of our products, services and data.</td>
</tr>
</tbody>
</table>

### Data Disclosure Example Language

<table>
<thead>
<tr>
<th>Exceeds Minimum Viable Privacy</th>
<th>Meets Minimum Viable Privacy</th>
<th>Does Not Meet Minimum Viable Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Licensor agrees that no personally identifiable information, including but not limited to log-ins recorded in system logs IP addresses of patrons accessing the system, saved searches, usernames and passwords, will be shared with third parties, except in response to a subpoena, court order, or other legal requirement. If Licensor is compelled by law or court order to disclose personally identifiable information of Authorized Users of patterns of use, Licensor shall provide the Licensee with adequate prior written notice as soon as is practicable, so that Licensee or Authorized Users may seek protective orders or other remedies.</td>
<td>The Licensor shall not, without the prior written consent of Subscriber, transfer any personal information of any Authorized User to any third party or use it for any purpose other than as described in this Agreement and in the online privacy policy for the relevant online service.</td>
<td>We shall not provide your usage statistics in any form to any third party without your written authorization, unless the third party owns rights in the products and services.</td>
</tr>
<tr>
<td>Raw usage data relating to the identity of specific users and/or uses shall not be provided to any third party.</td>
<td>The Licensor shall not disclose or sell usage data or information about the Licensee or its Authorized Users without the Licensee’s written permission.</td>
<td>We may use this information to test and improve our products and services and to protect and enforce our rights under the agreement and may pass this information to our third party providers for the same purposes.</td>
</tr>
<tr>
<td>Exceeds Minimum Viable Privacy</td>
<td>Meets Minimum Viable Privacy</td>
<td>Does Not Meet Minimum Viable Privacy</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Raw usage data, including but not limited to information relating to the identity of specific users and/or uses, shall not be provided or sold to any third party.</td>
<td>Licensor shall not, without the prior written consent of the Licensee(s) transfer any personal information of any Authorized Users to any affiliated and/or non-affiliated third party or use it for any purpose except as is necessary to perform the Services in compliance with applicable State &amp; Federal laws and institutional regulations, including the Family Educational Rights and Privacy Act (“FERPA”).</td>
<td></td>
</tr>
</tbody>
</table>

**Data Processing Example Language**

<table>
<thead>
<tr>
<th>Exceeds Minimum Viable Privacy</th>
<th>Meets Minimum Viable Privacy</th>
<th>Does Not Meet Minimum Viable Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor shall not use the Personal Information for any purpose except in the performance of this Agreement and to provide Support Services to the Participating Institutions and their respective permitted users. Vendor will not use the Customer Data (including metadata) for advertising or marketing purposes unless such use is specifically authorized by the applicable Participating Institution. Vendor is prohibited from Mining Customer Data for any purposes other than as part of the normal functioning of the Service for the benefit of Participating Institution and the operation of the Services environment by Vendor or those otherwise agreed to by the applicable Participating Institution.</td>
<td>Such usage data shall be compiled in a manner consistent with applicable privacy and data protection laws, and the anonymity of individual users and the confidentiality of their searches shall be fully protected.</td>
<td>For the sake of clarity, the storage of personal data in a third-party environment will not be deemed “sharing” for the purposes of this section.</td>
</tr>
</tbody>
</table>
### Vendor Privacy Policy Example Contract Language

<table>
<thead>
<tr>
<th>Exceeds Minimum Viable Privacy</th>
<th>Meets Minimum Viable Privacy</th>
<th>Does Not Meet Minimum Viable Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Except as otherwise expressly provided for in this Agreement, our Service is subject to [vendor] Privacy Policy, which is expressly made a part of this Agreement as Appendix A.</td>
<td>In the event that Licensor requires Authorized Users to agree to terms relating to the use of the Licensed Materials before permitting Authorized Users to gain access to the Licensed Materials (commonly referred to as “click-through” licenses), or otherwise attempts to impose such terms on Authorized Users through mere use or viewing of the Authorized Materials, Licensor shall provide Licensee with notice of and an opportunity to comment on such terms prior to their implementation. In no event shall such terms materially differ from the provisions of this Agreement.</td>
<td>Our products and services may include data, software and services from third parties. Some third party providers require us to pass additional terms through to you. The third party providers change their terms occasionally and new third party providers are added from time to time. To see the current third party additional terms for our products and services visit [URL].</td>
</tr>
</tbody>
</table>

### Data Ownership Example Language

<table>
<thead>
<tr>
<th>Exceeds Minimum Viable Privacy</th>
<th>Meets Minimum Viable Privacy</th>
<th>Does Not Meet Minimum Viable Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participating Institutions retain ownership of the Personal Information of each and may, at any time during the term of this Subscription Agreement, access, review, modify and delete Personal Information that Vendor is storing.</td>
<td>Licensor does not own any data, information or material that you submit to the Software (“Customer Data”).</td>
<td>Vendor may derive insights from its processing, aggregation, and analysis of data submitted by Client. The parties hereby agree that Vendor shall have the right to use, apply, and disseminate any such insights as it sees fit.</td>
</tr>
<tr>
<td>Exceeds Minimum Viable Privacy</td>
<td>Meets Minimum Viable Privacy</td>
<td>Does Not Meet Minimum Viable Privacy</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>In the case that the Publisher assigns its rights to another party, the Licensee may at its discretion require the assignee either to keep such usage information confidential or to destroy it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>After termination and upon request, Vendor will promptly return or destroy all applicable Institution Data, except however, Vendor may retain Institution Data in back-up files provided that the confidentiality and security obligations contained herein shall apply.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**User Surveillance Example Language**

<table>
<thead>
<tr>
<th>Exceeds Minimum Viable Privacy</th>
<th>Meets Minimum Viable Privacy</th>
<th>Does Not Meet Minimum Viable Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>This licensor shall not require the use of an authentication system that creates an unnecessary barrier to authorized access by users.</td>
<td></td>
<td>Vendor may derive insights from its processing, aggregation, and analysis of data submitted by Client. The parties hereby agree that Vendor shall have the right to use, apply, and disseminate any such insights as it sees fit.</td>
</tr>
</tbody>
</table>

**Data Security and Accountability Example Language**

<table>
<thead>
<tr>
<th>Exceeds Minimum Viable Privacy</th>
<th>Meets Minimum Viable Privacy</th>
<th>Does Not Meet Minimum Viable Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor will promptly notify Institution in the event of a verified breach of non-public personal data unless such breach is unlikely to result in material harm to Institution or the data subject, or as otherwise provided by law. Institution agrees that it shall be Institution’s sole responsibility to determine</td>
<td>Licensor will notify Licensee and Authorized Users as soon as is practicable if the Licensor’s systems are breached and the confidentiality of personally identifiable information is compromised.</td>
<td>In no event shall Vendor or its suppliers be liable for any incidental or consequential damages, lost profits or lost data, or any other indirect damages caused by Vendor performance or nonperformance of this Agreement, except where such damages</td>
</tr>
<tr>
<td>Exceeds Minimum Viable Privacy</td>
<td>Meets Minimum Viable Privacy</td>
<td>Does Not Meet Minimum Viable Privacy</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>whether a breach is subject to state, federal or national breach notification laws and requires breach notification (“Breach Notification”). In the event that Institution determines that a breach requires Breach Notification, Vendor agrees that it will reasonably cooperate with Institution in regards to Institution’s Breach Notification obligations as specified in the applicable law, including Institution’s investigation, enforcement, monitoring, document preparation, Breach Notification requirements, and reporting.</td>
<td></td>
<td>arise through Vendor failure to take reasonable precautions.</td>
</tr>
<tr>
<td>Vendor publishes or makes available its information security procedures (“Information Security Plan”) to Licensee and its other customers and regularly reviews its Information Security Plan and updates and revises from time to time as necessary. Vendor shall perform an annual audit by a third-party independent auditor of its compliance with the ISO-27001 (or comparable industry) standard.</td>
<td>Vendor will maintain current data security management practices that follow established standards and will notify Licensee in the event of any data breach occurring.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vendor will (i) implement administrative, physical, and technical safeguards in accordance with accepted industry practices including conducting audits in accordance with the ISO/IEC 27001 standard (or subsequent comparable standard) and (ii) as reasonably requested by Institution, provide Institution with a copy of the certificate of registration for such standard along with any relevant reported deficiencies regarding non-compliance together with corrective action plans for addressing such deficiencies identified in the report.</td>
<td></td>
</tr>
</tbody>
</table>
Licensing Privacy - Vendor Contract and Policy Rubric

Vendor name:
Name of product/service:
Review date:
Reviewer name:

Licensing Privacy Project
https://publish.illinois.edu/licensingprivacy/
The Vendor Contract and Privacy Rubric was developed by LDH Consulting Services as a component of the Licensing Privacy project led by Lisa Janicke Hinchliffe. This project was made possible in part by The Andrew W. Mellon Foundation.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

Cover photo credits: DLKR on Unsplash
About This Rubric

Scope
This rubric evaluates data privacy criteria in content platform vendor contracts and privacy policies. This rubric aims to assist libraries in identifying potential data privacy risks so that libraries can determine how to address these risks with vendors.

This rubric does not measure compliance to library privacy or data privacy legal regulations such as GDPR, FERPA, or other federal and state laws. Please consult with legal staff to review vendor contracts for compliance to specific regulations. Libraries interested in an in-depth review of technological standards and practices around data privacy, security, and identify management are encouraged to collaborate with their IT department or technology staff.

Privacy Level Definitions

Minimum Viable Privacy (MVP) is the consensus of library patron data privacy standards, guidelines, and practices from ALA, ILFA, and NISO. The specific standards used to create this rubric, along with more information about the rubric’s creation, can be found at https://publish.illinois.edu/licensingprivacy/.

Exceeds Minimum Viable Privacy
Vendor consistently goes above and beyond the MVP practices and standards.

Meets Minimum Viable Privacy
Vendor consistently meets MVP practices and standards.

Does Not Meet Minimum Viable Privacy
Vendor does not address privacy practices or current practices do not meet MVP practices and standards.

A vendor meeting or exceeding MVP in a specific privacy domain does not necessarily mean that the vendor is adequately protecting patron privacy. While librarianship strives to protect privacy, the above professional standards do not reflect the full spectrum of privacy risks patrons face in their use of the library, particularly patrons in minoritized groups. These professional standards also do not reflect the most current and comprehensive set of data privacy practices and risks. Library workers should assess the evolving risk in each privacy domain when determining the level of privacy that is most appropriate for their patrons based on potential harm if a particular privacy risk is realized.

Tips in Evaluating the Vendor Contract and Privacy Policy

- The three privacy levels serve as a guide for library workers to identify potential privacy risks in key data privacy domains in the vendor contract and privacy policy. There is no final score; nonetheless, a library must take considerable care in negotiations with a vendor that has a significant amount of contract language or practices that fall in the “Does Not Meet Minimum Viable Privacy” level.
- Data privacy practices can vary widely within a business; therefore, a vendor might be strong in one data privacy domain and weak in another.
- Vendor contracts and policies might not neatly fit into one level, but instead have language or practices that fall into two or all three levels. It is up to the library to determine how to proceed in addressing the risks present in that particular privacy domain.
- Sometimes the scope of the privacy policy posted on the vendor website does not pertain to the specific product or service under review. Ask the vendor if there is a privacy policy specific for the product or service if you are unsure about the scope of the posted policy.
On The Relationship Between Vendor Contract and Privacy Policy

Content provider contracts and licenses typically include very little detail about patron data privacy and security. Vendor privacy policies and terms of use fill in these knowledge gaps and give both library and patron more information about vendor privacy practices. This rubric includes both the contract and the policy in reviewing vendor privacy practices, but library workers must be aware of the nature of the relationship between the two documents. A contract is a legal document that carries obligations and responsibilities, as well as consequences if the terms of the contract are breached. While a privacy policy can be considered a legal document, there might be little recourse for libraries when a vendor changes its privacy policy if the contract lacks a clause for re-negotiation of the contract following major privacy policy changes.

Vendor contracts that have neither comprehensive explanation of data privacy practices nor an indication of a review-comment-notification process when there is a major privacy policy change puts patron privacy at risk. Library workers must negotiate such contracts with care, including adding model language around data privacy practices or language around when there is a major change to the vendor privacy policy.

Before You Begin

Take some time to gather the following documents before starting work on the rubric:

- Vendor contract and privacy policy
- Library patron privacy and confidentiality policies
- Organizational data privacy and confidentiality policies
- Glossary [https://publish.illinois.edu/licensingprivacy/glossary]
- Example contract language [https://publish.illinois.edu/licensingprivacy/example-contractlanguage]

Tips for Using the Rubric Form

- Each privacy domain page has a rubric table, notes section, and risk section. The notes and risk sections are text fields that can be filled out and saved to the document.
- You can check multiple boxes in a single privacy level, as well as across privacy levels in a single privacy domain, if you wish to use these criteria lists as checklists.
- You can complete the fields in the title page to autofill the footer and header throughout the rubric form. This will be useful to keep track of multiple documents if you are using the rubric to review multiple vendor contracts.
- Any criteria selected in the “Does Not Meet Minimum Viable Privacy” list for any privacy domain will be automatically listed in the “Does Not Meet Minimum Viable Privacy - Areas of Concern” section.
## Data Collection

*What data does the vendor collect, how and where do they collect data, and what is the rationale for collecting it?*

<table>
<thead>
<tr>
<th>☐ Exceeds Minimum Viable Privacy</th>
<th>☐ Meets Minimum Viable Privacy</th>
<th>☐ Does Not Meet Minimum Viable Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Follows data minimization practices.</td>
<td>☐ Provides a list of data collected and the business purpose for collection.</td>
<td>☐ Collects user data without indicating the business needs for said data.</td>
</tr>
<tr>
<td>☐ Provides clear explanation about what personal and non-personal data is collected and the business purpose for collection.</td>
<td>☐ Users can opt in/out of non-essential data collection.</td>
<td>☐ Does not list data collected from users.</td>
</tr>
<tr>
<td>☐ Collects personal data only after obtaining explicit and informed consent from users.</td>
<td>☐ Does not collect biometric information.</td>
<td>☐ Users are by default opted into non-essential data collection.</td>
</tr>
<tr>
<td>☐ Does not require personal data for authentication or authorization.</td>
<td>☐ Does not collect personal data to use the core features of the product.</td>
<td>☐ Requires users to provide personal data to use core features of the product.</td>
</tr>
<tr>
<td>☐ Does not require library to send user personal data beyond what is absolutely needed for authorization or authentication.</td>
<td>☐ Does not require library to send user personal data for authentication or authorization to use the product.</td>
<td></td>
</tr>
</tbody>
</table>

### Notes

Add notes here

### Data Collection Risks

*What are the major patron privacy risks in this domain?*

List risks here

*How can we address these risks?*

List ideas here
# User Data Rights

*What controls do users have over the vendor’s ability to collect, retain, use, and share user data?*

<table>
<thead>
<tr>
<th>☐ Exceeds Minimum Viable Privacy</th>
<th>☐ Meets Minimum Viable Privacy</th>
<th>☐ Does Not Meet Minimum Viable Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Users can access, modify, export, and delete their data at any time.</td>
<td>☐ Users can access, modify, and delete their data at any time.</td>
<td>☐ Users cannot access, modify, export, or delete their data with the vendor.</td>
</tr>
<tr>
<td>☐ Users can opt in/out of non-essential data collection, processing, and disclosure at any time, with vendor retroactively deleting user data upon opt out.</td>
<td>☐ Users can opt in/out of non-essential data collection, processing, and disclosure to third parties at any time.</td>
<td>☐ Users cannot opt out of non-essential data collection, processing, and disclosure at any time.</td>
</tr>
</tbody>
</table>

# Notes

Add notes here.

# User Data Rights Risks

*What are the major patron privacy risks in this domain?*  
*How can we address these risks?*

List risks here  
List ideas here
Data Disclosure

**What data does the vendor share and with which parties? Why is the data shared, and how is data sharing controlled/determined?**

<table>
<thead>
<tr>
<th>Exceeds Minimum Viable Privacy</th>
<th>Meets Minimum Viable Privacy</th>
<th>Does Not Meet Minimum Viable Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Clearly explains what personal data is disclosed to specific third parties and provides business cases for disclosure.</td>
<td>☐ Describes what data is disclosed to third parties and business cases for disclosure.</td>
<td>☐ Does not list what data is disclosed to third parties.</td>
</tr>
<tr>
<td>☐ Does not disclose personal data to law enforcement unless under court order.</td>
<td>☐ Does not disclose personal data to law enforcement unless under court order.</td>
<td>☐ Discloses user data to third parties without providing users an option to opt out.</td>
</tr>
<tr>
<td>☐ Does not disclose or sell user data to data brokers and advertisers.</td>
<td>☐ Users can opt-in to data sharing with third parties.</td>
<td>☐ Does not have a law enforcement request policy or the policy contradicts library and organizational policies.</td>
</tr>
<tr>
<td>☐ Aggregates or otherwise de-identifies data before disclosing to third parties.</td>
<td>☐</td>
<td>☐ Discloses or sells user data to advertisers or data brokers.</td>
</tr>
</tbody>
</table>

**Notes**

Add notes here

Data Disclosure Risks

**What are the major patron privacy risks in this domain?**

List risks here

**How can we address these risks?**

List ideas here
## Data Processing

*What data does the vendor use, for what purpose, and how is data use controlled/determined?*

<table>
<thead>
<tr>
<th>☐ Exceeds Minimum Viable Privacy</th>
<th>☐ Meets Minimum Viable Privacy</th>
<th>☐ Does Not Meet Minimum Viable Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides clear explanation about processes that involve user data.</td>
<td>Provides explanation about data processing needs and practices.</td>
<td>Does not explain data processing needs or practices.</td>
</tr>
<tr>
<td>Explains use of rigorous data de-identification methods.</td>
<td>Aggregates personal data after a designated time.</td>
<td>Retains personal data in perpetuity.</td>
</tr>
<tr>
<td>Does not use personal data for marketing or advertising purposes.</td>
<td>Deletes individual user data when no longer needed for operational purposes.</td>
<td>Repurposes user data without explicit consent from users.</td>
</tr>
<tr>
<td></td>
<td>Only repurposes data when user gives explicit and informed consent.</td>
<td>De-identification methods are weak or not suitable for the data set.</td>
</tr>
<tr>
<td></td>
<td>Defines de-identification methods.</td>
<td>Uses “anonymization” without defining methods used to “anonymize” data.</td>
</tr>
</tbody>
</table>

### Notes

Add notes here

### Data Processing Risks

**What are the major patron privacy risks in this domain?**

List risks here

**How can we address these risks?**

List ideas here
Privacy Policy
What public privacy statements are available on the vendor’s service or website? Are any internal vendor privacy policies provided to the library?

<table>
<thead>
<tr>
<th>☐ Exceeds Minimum Viable Privacy</th>
<th>☐ Meets Minimum Viable Privacy</th>
<th>☐ Does Not Meet Minimum Viable Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Includes full text of privacy policy in contract or indicates their obligations to work with libraries when there are updates to the publicly posted notice.</td>
<td>☐ Has a publicly available privacy policy that the public can access on the vendor site.</td>
<td>☐ Does not have a publicly available privacy policy.</td>
</tr>
<tr>
<td>☐ Data protections go beyond those in library and/or organizational policies.</td>
<td>☐ Policy is written in clear, concise language for a general audience, describing the lifecycle of user data collected by vendor.</td>
<td>☐ If there is a privacy policy, vendor gives no recourse for libraries to renegotiate contract terms when there are updates to the policy.</td>
</tr>
<tr>
<td></td>
<td>☐ Data protections roughly match protections in the library and/or organizational policies.</td>
<td>☐ Library or organizational privacy policies provide substantial privacy protections over the vendor policy.</td>
</tr>
<tr>
<td></td>
<td>☐ Notifies library of changes to policy and renegotiate contract terms if necessary.</td>
<td></td>
</tr>
</tbody>
</table>

Notes
Add notes here

Privacy Policy Risks
What are the major patron privacy risks in this domain? How can we address these risks?

List risks here
List ideas here
Data Ownership

Who owns the data in the vendor service or product and what rights come with data ownership in specific business scenarios?

<table>
<thead>
<tr>
<th>☐ Exceeds Minimum Viable Privacy</th>
<th>☐ Meets Minimum Viable Privacy</th>
<th>☐ Does Not Meet Minimum Viable Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Library retains the right to withdraw data in the case of mergers, acquisitions, and bankruptcies.</td>
<td>Vendor retains ownership of user data. Vendor deletes user data when the business relationship ends. Vendor notifies users about option to delete data after acquisition or merger.</td>
<td>Vendor retains ownership of user data, even after the end of the business relationship or in the case of mergers, acquisitions, and bankruptcies.</td>
</tr>
<tr>
<td>Vendor deletes all user data, including in the aggregate, when the business relationship ends.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Notes

Add notes here

Data Ownership Risks

What are the major patron privacy risks in this domain? How can we address these risks?

List risks here
List ideas here
### User Surveillance

What tracking or logging mechanisms does the vendor use to collect user data, and what level of control do users have over vendor tracking/logging behavior while using the service?

<table>
<thead>
<tr>
<th>□ Exceeds Minimum Viable Privacy</th>
<th>□ Meets Minimum Viable Privacy</th>
<th>□ Does Not Meet Minimum Viable Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Does not use web analytics or other types of digital surveillance methods to track users in and beyond the vendor website or service.</td>
<td>□ Gives users an option to opt in/out of web cookies or other web tracking methods for personalization features of product.</td>
<td>□ Tracks users on their website without consent or an option to opt out of tracking.</td>
</tr>
<tr>
<td>□ Does not collect or store data on user search and content access histories by default.</td>
<td>□ Does not require users to create a separate account that requires the collection of additional user data to use the service.</td>
<td>□ Uses tracking methods to track users outside of the vendor service.</td>
</tr>
<tr>
<td>□ Does not engage in behavioral tracking of user activity on or outside the service or product.</td>
<td>□ User can opt in/out of saving content access and search histories at any time.</td>
<td>□ Engages in behavioral tracking of user activity by default.</td>
</tr>
<tr>
<td>□ Does not require users to create a separate account that requires the collection of additional user data to use the service.</td>
<td>□ Reserves the right to deny users access to content based on collected behavioral data such as subject or topic area of content accessed.</td>
<td>□ Reserves the right to deny users access to content based on collected behavioral data such as subject or topic area of content accessed.</td>
</tr>
</tbody>
</table>

### Notes

Add notes here

### User Surveillance Risks

What are the major patron privacy risks in this domain? How can we address these risks?

List risks here

List ideas here
## Data Security and Accountability

How does the vendor protect data in transit and in storage from unauthorized access or use? How does the vendor prevent and respond to data breaches or leaks?

What checks are in place to ensure compliance to security and privacy policies and standards?

<table>
<thead>
<tr>
<th>☐ Exceeds Minimum Viable Privacy</th>
<th>☐ Meets Minimum Viable Privacy</th>
<th>☐ Does Not Meet Minimum Viable Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Clearly describes data security practices, including encryption methods, purpose limitation, and access controls to user data.</td>
<td>☐ Describes general data security practices.</td>
<td>☐ Does not describe data security practices.</td>
</tr>
<tr>
<td>☐ Contracts with independent third party to conduct data security and privacy audits.</td>
<td>☐ Encrypts data in transit and in storage.</td>
<td>☐ Does not proactively conduct annual data security and privacy audits.</td>
</tr>
<tr>
<td>☐ Clearly states incident response plan and responsibilities, including user notification.</td>
<td>☐ Conducts annual data security and privacy audits.</td>
<td>☐ Does not have an incident response plan, including user notification plan.</td>
</tr>
</tbody>
</table>

### Notes

Add notes here

### Data Security and Accountability Risks

What are the major patron privacy risks in this domain?  How can we address these risks?

List risks here  List ideas here
Does Not Meet Minimum Viable Privacy - Areas of Concern

The following list comes from the items marked in the “Does Not Meet Minimum Viable Privacy” level from every privacy domain in the rubric. Libraries are strongly advised to address these risks during vendor selection and contract negotiation processes.

Tip: Libraries can reference the model language at https://publish.illinois.edu/licensingprivacy/ in mitigating the risks listed below.

Data Collection

User Data Rights

Data Disclosure

Data Processing

Data Ownership

User Surveillance

Data Security and Accountability