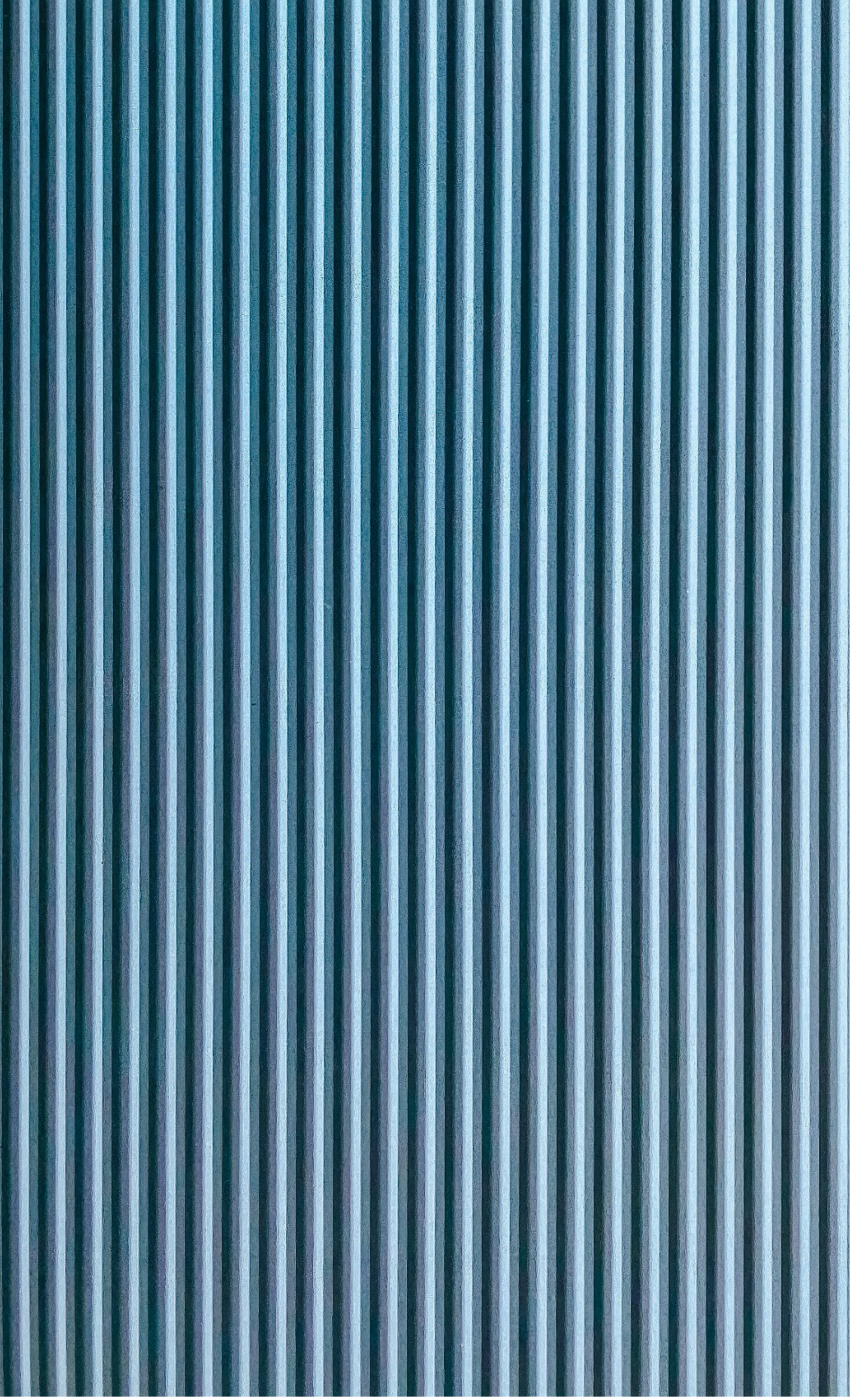

Licensing Privacy - Vendor Contract and Policy Rubric

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.

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 explanations 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-contract-language]

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?

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

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?

☐ Exceeds Minimum Viable Privacy	**☐ Meets Minimum Viable Privacy**	**☐ Does Not Meet Minimum Viable Privacy**
☐ Users can access, modify, export, and delete their data at any time. ☐ 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.	☐ Users can access, modify, and delete their data at any time. ☐ Users can opt in/out of non-essential data collection, processing, and disclosure to third parties at any time.	☐ Users cannot access, modify, export, or delete their data with the vendor. ☐ Users cannot opt out of non-essential data collection, processing, and disclosure at any time.

Notes

Add notes here

User Data Rights Risks

What are the major patron privacy risks in this doman?

List risks here

How can we address these risks?

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?

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

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?

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

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?

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

Notes

Add notes here

Privacy Policy Risks

What are the major patron privacy risks in this domain?

List risks here

How can we address these risks?

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?

□ **Exceeds Minimum Viable Privacy**	□ **Meets Minimum Viable Privacy**	□ **Does Not Meet Minimum Viable Privacy**
□ Library retains the right to withdraw data in the case of mergers, acquisitions, and bankruptcies. □ Vendor deletes all user data, including in the aggregate, when the business relationship ends.	□ Library 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.	□ Vendor retains ownership of user data, even after the end of the business relationship or in the case of mergers, acquisitions, and bankruptcies.

Notes

Add notes here

Data Ownership Risks

What are the major patron privacy risks in this domain?

List risks here

How can we address these risks?

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?

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

Notes

Add notes here

User Surveillance Risks

What are the major patron privacy risks in this domain?

List risks here

How can we address these risks?

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?

□ **Exceeds Minimum Viable Privacy**	□ **Meets Minimum Viable Privacy**	□ **Does Not Meet Minimum Viable Privacy**
□ Clearly describes data security practices, including encryption methods, purpose limitation, and access controls to userdata. □ Contracts with independent third party to conduct data security and privacy audits. □ Clearly states incident response plan and responsibilities, including user notification.	□ Describes general data security practices. □ Encrypts data in transit and in storage. □ Conducts annual data security and privacy audits. □ Maintains data privacy and security training for staff. □ Indicates user notification responsibilities after a data breach or leak.	□ Does not describe data security practices. □ Does not proactively conduct annual data security and privacy audits. □ Does not have an incident response plan, including user notification plan.

Notes

Add notes here

Data Security and Accountability Risks

What are the major patron privacy risks in this domain?

List risks here

How can we address these risks?

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

Privacy Policy

Data Ownership

User Surveillance

Data Security and Accountability