Privacy Language Primer

Library licensed information resources are usually accessed through the vendors' platform. As librarians, we have two main ways to help protect our users from unreasonable intrusion or surveillance: 1) alerting our users to the existence of vendors' online terms of use and privacy policies, and 2) protecting our users' rights and data through the language included in the vendor licensing agreements. Negotiating strong privacy protection language in these agreements helps us preclude a vendor from sharing, selling, or exploiting user personally identifiable information.

The terms ‘privacy’ and ‘confidentiality’ can mean different things in different contexts, and strict attention should be paid to the ways they can surface in our agreements, and to the intentions of the language. For example, we want to ensure the vendor treats patron usage of their content as ‘confidential’, but we want to discourage vendors from keeping their pricing models and licensing terms and practices ‘confidential’.

For example, some of the terms we are looking to assert will:

- Maintain the confidentiality of all user data and activity on a vendor’s platform
- Prohibit data brokering and surveillance
- Limit data gathering and use to the performance of the service
- Prohibit linked out terms and end user license agreements (EULAs)
- Require usage data to be anonymized and aggregated
- Comply with applicable laws and regulations such as FERPA and GDPR

So where does this language occur in license agreements? Each agreement is different, and the language and sequence of terms will vary according to the concerns of the particular vendor supplying the license. Privacy terms can appear throughout the license. Below are some examples of sections and clauses containing privacy language, and what the language is meant to convey. The examples are pulled from existing agreements and have been edited for clarity and anonymized. They include the following:

1. Definitions
2. Usage Data Clauses
3. Data Privacy and Security
4. Confidentiality Clauses
5. References to Data Protection Laws
6. Linked Out Terms and Conditions, Privacy Policies
7. Data Processing Addendum
8. Using Model Language

1. Definitions

Some agreements include a Definitions section or glossary in the first section, and various terms relating to privacy and confidentiality can usually be found here. Some are included as concerns of the vendor and some as concerns of the licensing library. For example:

> **Authorized users** include those persons affiliated with Licensee as students, faculty, staff, and independent contractors of Licensee and its participating institutions, regardless of the physical location of such persons, as well as walk-in users.

These are the users we are authenticating to the data on the vendor platform, and whose personal data the library is concerned about protecting.

> **Access** Licensee shall maintain the confidentiality of any institutional passwords provided by Licensor.

Access is an example of concern about confidentiality from the vendor's side.

> **Applicable Laws** means all statutes, laws, rules, regulations, ordinances, and the like of any federal, international, city, state, provincial, or local government or governmental agency applicable to Services under the Agreement including without limitation Data Protection Laws.

Applicable Laws will be referenced in language about the vendor's obligations to user data privacy.

> **Intellectual Property**: Together with our licensors, we retain all ownership of and all rights in our products (including any underlying data model, database or data set) and any configurations or modifications to our products ("our property"). Our property constitutes our valuable intellectual property, confidential information and trade secrets, and you may only use it as expressly permitted in the agreement. You must promptly notify us if you become aware of any unauthorized use of our property.

The above text box is an example of the vendor merging their information (which may include license language and pricing) into a larger idea of intellectual property and copyright, and requesting confidentiality.

> **Secure Network**: A network that is only accessible to Authorized Users approved by the Licensee and whose identities are authenticated at the time of login and whose conduct is subject to review and regulation by the Licensee. Such secure networks may include proxy servers maintained and controlled by the Licensee.

The secure network will occasionally be cited as a means to protect confidentiality for both parties.

> **Third party providers.** The Products may include data, software and services from third parties. Some third party providers require [Vendor] to pass additional terms through to you, and you must comply with these additional terms as applicable. The third party providers change their terms occasionally and new third party providers are added from time to time.

Language regarding third parties can introduce risk to user privacy, as personally identifiable information can be disclosed and used. Language that protects against third party access to user data would improve the section.

2. Usage Data Clauses

Vendors should provide usage data for the products being licensed, compliant with the latest release of the COUNTER Code of Practice. Usage data clauses are therefore another location in a license in which it is common to find terms regarding privacy and confidentiality. In this case, privacy means the protection of the personally identifiable information that becomes available to the vendor as our library users access, search, and engage with the vendor's platform and content.

However, there is a risk that vendors can use the data they gather for purposes beyond reporting usage – purposes that may include marketing or selling that data to third parties. To minimize that risk, vendors should be required through the license terms to anonymize and aggregate their usage data, and they should be precluded from sharing that data with third parties.

These clauses will often appear under Licensor Responsibilities.

> **Example 1:** Licensor will make available to the Licensee monthly usage reports throughout the Publication Term for each Publication, detailing the level of use of each Publication by the Licensee's Authorized Users per month. The Publisher shall use reasonable efforts to ensure that such usage reports are compliant with the most recent release of the COUNTER Code of Practice for Journals and Databases.

In this example, there is no acknowledgement by the vendor of the need to keep the usage data confidential, and there is a risk they may share it with third parties.

> **Example 2:** Publisher agrees to maintain the confidentiality of any data relating to the usage of the Licensed Materials by the Licensee and its Authorized Users. Such data may be used solely for purposes directly related to the Services and may only be provided to third parties in aggregate form. Raw usage data, including but not limited to information relating to the identity of specific users and/or uses, shall not be provided to any third parties.

This example is much better. It protects the confidentiality of all usage, and specifically protects personally identifying information and individual use by preventing its being shared with any third parties. (See #8 below for model language.)

3. Data Privacy and Security

Some agreements will have separate sections dedicated to data privacy and security, but the presence of these sections alone does not guarantee privacy or protection of user data. They must be read closely to ensure the confidentiality they are trying to protect is that of the users and not simply that of their licensed materials.

> **Example 1:** To the extent that [Vendor] processes personal data (as that term is defined under applicable law) pursuant to this Agreement it shall do so in accordance with its Privacy Policy available at [link]. For the avoidance of doubt, [Vendor] is and shall remain the controller (or similar term under applicable law) of personal data processed under this Agreement. Licensor agrees to maintain the confidentiality of any data relating to the usage of the licensed content by Licensee and its Authorized Users. Such data may be used solely for providing access to the licensed content under this agreement and may only be provided to third parties in aggregate, anonymized form, and only with prior notice to and consent from Licensee. Licensor will not incorporate data from authorized use of resources licensed under this agreement in products sold to third parties, including governments, to facilitate surveillance, "threat assessment," or for any other purpose. Raw usage data, including but not limited to information relating to the identity of specific users and/or uses, shall not be provided to any third party 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 or 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. 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. The Licensor 's obligations under this clause will survive the expiration or other termination of this agreement.

This language contains strong protections for the privacy of user data. The Licensor agrees to maintain confidentiality of usage data and agrees not to share it with third parties. It even specifies that it will not facilitate surveillance or threat assessment. But it also points to their online privacy policy, which introduces risk. (See #6 below for model language.)

4. Confidentiality Clauses

Many agreements include a separate clause for Confidentiality. They may be brief, or they may be thorough, including a definition of confidential information and a description of how it should be handled. But the inclusion of a confidentiality clause should not be confused with privacy protections.

> **Example 1: *Confidentiality.*** Confidential information shall not include information that is public record pursuant to [state] law ([state] Statutes Chapter [#]. This provision shall survive termination of the Agreement.

This is the extent of the vendor's consideration of confidentiality. It says nothing about how they will treat user data.

> **Example 2:** Each Party acknowledges that, in connection with the performance of this License Agreement, it may receive certain confidential or proprietary technical, business or financial information and materials of the other Party or data related to the usage of the Licensed Materials by Licensee and Authorized Users ("Confidential Information"). Confidential Information shall include the disclosing Party's service offerings, methodologies, software, product documentation, data, legal strategies and work product, and any other business, financial or technical information that is marked or otherwise identified as confidential or proprietary. Confidential Information includes the License Fees charged by the [Vendor] for the Licensed Materials and the terms of this License Agreement as signed to by the [Vendor] and the Licensee's designated representative authorized to bind the Licensee to this License Agreement.
>
> Both Parties agree (a) to use the other Party's Confidential Information only for the purposes described in this License Agreement; (b) not to reproduce the other Party's Confidential Information and will hold in confidence and protect such Confidential Information from dissemination to, and use by, any third party; and (c) to restrict access to the other Party's Confidential Information to such of its personnel, agents, suppliers and/or consultants, if any, who have a need to have access and who have been advised of and have agreed in writing to treat such information in accordance with the terms of this License Agreement. Both Parties agree that all Confidential Information is proprietary to the disclosing Party or such third party, as applicable, and shall remain the sole property of the disclosing Party or such third party.

This example is better at protecting user privacy, keeping data confidential and not sharing with third parties. In the first paragraph, "confidential information" is defined. The definition includes information shared between the Parties, but it also includes the pricing and terms of the agreement. The second paragraph asserts mutual confidentiality, suggesting that if we want to assure confidentiality of our user data, we must also keep the pricing and terms of the agreement confidential. This language can be improved by excluding the agreement terms and pricing from Confidential Information. (See #8 below for model language.)

Another concern arises where the vendor asks that the pricing and terms of the agreement remain confidential. Opaque pricing models and confidentiality of license terms do not serve the interest of academic libraries and lead to unfairness in the marketplace. Consider deleting these clauses:

> **Model language: *Confidentiality*:** INTENTIONALLY DELETED

5. References to Data Protection Laws

In 2016 the EU adopted the General Data Protection Regulation (GDPR), and full implementation was required by 2018. GDPR has become a common standard for data privacy protection, and many vendors will include language referencing it somewhere in their agreements - particularly those based in the EU, or with offices there. The GDPR provides detailed rules around the processing of personal data, including the right to be forgotten.

Example 1: The Supplier shall ensure that all personal data is properly collected, stored, processed, secured, archived or destroyed in compliance with Federal, State and applicable international privacy laws, including the EU General Data Protection Regulation 2016/679 (GDPR).
Example 2: Both Parties represent and warrant that a) it has the legal authority to enter into this License Agreement; b) this License Agreement will not conflict with any other contract, agreement or law; c) this License Agreement, executed and delivered, will constitute a binding obligation; and d) it shall adhere to Section 5 herein and all applicable privacy and data protection laws applicable to the gathering, processing, storing and transmitting of all confidential information, such as identifiable user information and other similar usage data.

The first example declares compliance with applicable laws, and cites GDPR specifically. In the second example, the vendor includes language about the adherence to data protection laws generally as part of the Warranties section, where the parties typically make representations about their mutual obligations. This language is more obvious and specific, and thus provides better protection.

6. Linked-out Terms and Conditions, Privacy Policies

Some agreements will contain language that refers to the vendor's online terms or posted privacy policy, a practice also known as link-outs. The online terms will also frequently contain language that allows the vendor to update them unilaterally at any time without notice. Referencing linked out documents introduces risk to the library that the terms may change unfavorably. Libraries can better protect users from this risk by insisting that all terms be contained within the agreement itself (including any addenda and appendices).

Example 1: Licensor hereby grants to Licensee an academic license to use and/or distribute the Product in the manner set forth in the Use and Distribution Section below, but subject to all limitations contained in this Exhibit A. In addition, Authorized Users accept the terms contained in the online Subscription and Use Agreement as may be amended from time to time at Licensor's discretion.

Linked-out terms introduce great risk, especially where the vendor claims unilateral right to change them. One option is to print the online terms and include them in the agreement.

> **Example 2:** To the extent that [VENDOR] processes personal data (as that term is defined under applicable law) pursuant to this Agreement it shall do so in accordance with its Privacy Policy available at [URL]

Links to online privacy policies also introduce risk. Such an agreement can be improved by including language that the vendor must maintain the confidentiality of all user information and usage data and will not give or sell it to third parties.

Another way to limit the risk is to add language to the license, or in an addendum, that nullifies linked out terms or end user license agreements. (See #8 below for model language.)

7. Data Processing Addendum

Some institutions will request the inclusion of a Data Processing Addendum with the agreement in order to secure the confidentiality of data being shared with the vendor. This is likely to include any personally identifiable information a vendor could gather from a user's activity on the vendor's platform.

> **Example 1:** Taking into consideration the state of the art, costs of implementation and the nature, scope, context and purposes of the Data Processing, the likelihood and potential severity of risks to the rights and freedoms of natural persons, and the risk of data breach, the Processor represents and warrants that it shall implement technical, physical, and administrative security measures appropriate to such risks, which may include, but are not necessarily limited to:
>
> 1. The de-identification, anonymization, pseudonymization, and encryption of [personal data];
> 2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems, facilities, and services;
> 3. The ability to restore the availability of and access to [personal data] in a timely manner in the event of a physical or technical incident; and
> 4. A process for regularly testing, assessing, and evaluating the effectiveness of technical, physical, and administrative measures for ensuring the security of the Data Processing.
>
> The processor's measures for protecting [personal data] shall a) meet or exceed industry best practices for safeguarding personal data, and (b) be based on the concepts of privacy by design and by default.

Note that the addendum language cites the "rights and freedoms" of users and highlights the risks associated with the availability of personal data. It requires the vendor to protect and keep confidential the personal data, and it even requires the vendor to address the maintenance of their systems to ensure the security of the data.

Example 2: ***Instructions.*** Institution instructs Vendor to Process Institution Personal Data solely as necessary to provide the Services to Institution as set forth in the Agreement and DPA, and for the other purposes expressly allowed in this DPA Vendor will inform Institution if, Vendor determines that it is no longer able to meet its obligations under Data Protection Laws or where in Vendor's reasonable opinion, any of Institution's instructions infringes any Data Protection Laws. Institution reserves the right to take reasonable and appropriate steps to ensure Vendor's Processing of Personal Data is consistent with Institution's obligations under Data Protection Law and discontinue and remediate unauthorized use of Personal Data.

Processing by Vendor. Vendor will Process Institution Personal Data in compliance with Data Protection Laws. For Institution Personal Data that Vendor Processes on behalf of Institution, Vendor will provide the same level of protection as required of Institution under Data Protection Laws. Vendor will not:

1. Sell or Share Institution Personal Data;
2. use, retain, or disclose Institution Personal Data outside of its direct business relationship with the Institution;
3. use, retain, or disclose Institution Personal Data for any other purpose (including any other commercial purpose) other than the Business Purpose, except as required or permitted by law; or
4. collect, use, retain or disclose more Institution Personal Data than is necessary for the purposes of providing the Services.
5. combine, reaggregate, or reidentify Institution Personal Data with Personal Data that it receives (a) from or on behalf of others, or (b) collects or Processes from Vendor's own interactions with Data Subjects provided that Vendor may combine Personal Data to perform any Business Purposes permitted or required under the Agreement to perform the Services.

Permitted Uses. Vendor may Process Institution Personal Data for:

6. The permitted purposes (including permitted Business Purposes) as described in Exhibit 1;
7. To create Aggregated Data to (a) operate, manage, test, maintain, and enhance the Services including as part of its internal business operations; (b) create and disclose aggregate statistics about the Services in a manner that prevents individual identification of Institution, or the individual subjects of Institution Personal Data.

In this example, the Data Processing Addendum language is specific about what the vendor may and may not do with the data. The vendor may improve the services, and provide aggregated usage, but they may not use the data in ways that introduce risk to a user's right to privacy.

8. Using Model Language

Most academic library agreements now have language regarding patron privacy and data security, but agreements from some smaller or new content providers may have no relevant language at all. Where no language exists to protect patron privacy, the vendor is free to use patron data as they like. It is our responsibility in managing our library's licenses to protect users from risk by introducing privacy language into these agreements. We may also thereby improve the vendor's future contracts.

The language below, suggested as part of the ASERL principles, contains very strong model language protecting user privacy and data security. It asserts the vendor maintains confidentiality of any data related to use of the products; it asserts only aggregated data can be shared with third parties, and only upon notice to and with consent of the Licensee; it asserts raw data cannot be provided to a third party unless via a legal requirement; and it prohibits use of data for surveillance purposes. Note that the language also includes survivability.

> **Model language from ASERL**: Licensor agrees to maintain the confidentiality of any data relating to the usage of the licensed content by Licensee and its Authorized Users. Such data may be used solely for providing access to the licensed content under this agreement and may only be provided to third parties in aggregate, anonymized form, and only with prior notice to and consent from Licensee. Licensor will not incorporate data from authorized use of resources licensed under this agreement in products sold to third parties, including governments, to facilitate surveillance, "threat assessment," or for any other purpose. Raw usage data, including but not limited to information relating to the identity of specific users and/or uses, shall not be provided to any third party 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 or 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. 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. The Licensor's obligations under this clause will survive the expiration or other termination of this agreement.

The model language below protects the institution from the risks of online terms and end user license agreements (EULAs):

> **EULA model language:** This [Agreement and Addendum] represent the entire agreement between [INSTITUTION] and [VENDOR]. In the event that [VENDOR] subsequently attempts to enter into terms of use agreements or other similar agreements, policies or understandings,

> whether on the Supplier's purchase order, website, click-through, verbal or in writing, with [INSTITUTION] employees or other end users, such agreements shall be null, void and without effect, and the terms of this Addendum and the Agreement shall apply. [INSTITUTION] will not be bound to any other terms and conditions set forth in any documents, agreements or policies unless such terms and conditions are also set forth in this Addendum and the Agreement. [VENDOR] may not unilaterally change any term or condition of this Addendum and the Agreement.

Summary

Most publishers and vendors with whom the academic library does business will provide their own standard license agreement for the library to review, and terms around privacy and confidentiality can occur throughout the agreement. Read agreements carefully to locate these terms, and edit or strike them as necessary. If there is a Definitions section, look for terms like *privacy, confidentiality, data security,* and *third parties*. Look for language on how usage statistics will be provided, and ensure usage data is either not shared, or at least anonymized and aggregated. Look for references to third-party vendors and protect against data sharing with them. Consider adding language to protect against linked out terms and online privacy policies. If your institution has its own data security policy or data processing addendum, add that language to your agreements. And where there is no language at all around privacy and confidentiality, keep in mind that means there are no protections for your users and their data and consider adding protective language to improve the agreement.