KPMG

Ex Libris
Pivot Privacy Impact Assessment

December 2019

1 - Table of Contents

2 - Disclaimer

This report is provided to Ex Libris Ltd. If this report is received by anyone other Ex Libris Ltd. The recipient is placed on notice that the attached report has been prepared solely for use in connection with Ex Libris Ltd. and this report and its contents may not be shared with or disclosed to anyone by the recipient without the express consent of Ex Libris Ltd. and KPMG Somekh Chaikin. KPMG Somekh Chaikin shall have no liability for the use of this report by anyone other than Ex Libris Ltd. and shall pursue all available legal and equitable remedies against recipient, for the unauthorized use or distribution of this report.

3 - Purpose of this document

The Privacy Impact Assessment (PIA) is a process that identifies what impact a project, initiative or general collection, and use of information might have on the privacy of individuals. A PIA is a point-in-time assessment, and the resultant report and other outputs should be revisited as changes occur to the processes that were originally assessed.

This PIA includes a brief description of the data processed in the Pivot service, the privacy impact, and the measures Ex Libris is taking in order to manage the risks involved.

4 - Main Findings and Conclusions

We have reviewed the privacy risks regarding Pivot and the privacy and security controls designed to mitigate those risks.

It should be noted that Ex Libris is a data processor, therefore, some of the personal data-relating processes are the responsibility of the data controller (Ex Libris customers), such as consent management.

Personal data in Pivot is limited in nature and the inherent risks resulting is low. The privacy controls designed and implemented comply with GDPR requirements, relating to the business processes of Pivot.

After reviewing all material GDPR aspects, the privacy risks, and implemented controls, any residual risk that we found was minimal. Our impression is that Ex Libris efforts in implementing GDPR requirements are well managed, resulting in a good level of compliance. Ex Libris has also appointed a Data Protection Officer (DPO).

One of the main principles of GDPR is Privacy by Design, which means promoting privacy principles throughout product and process development from the start, and maintaining this while products and services are developing. In order to maintain compliance, Ex Libris will need to continue their practice of making the privacy of its customers a core value, and lead by example for other SaaS vendors in the market.

5 - Scope and Plan

This PIA scope is Pivot, where Ex Libris is the data processor. The purpose for data processing is to accelerate the research process by integrating funding, collaborator discovery, and publishing opportunities into one tool for Ex Libris customers.

6 - Data Elements

Data needed for processing – information about the data subjects (library patrons) are provided by the Ex Libris customer (library authority). Additional personal data updates are done by the library staff when needed, and the processes involved are the sole responsibility of the library, which is the data controller.

Following is a list of data elements related to the data subject (patron), processed by Pivot. None of the data elements is encrypted in the database. All of the data elements are related to the patron:

Category	Data field	Mandatory
General Information	First Name	Yes
	Middle Name	No
	Last Name	Yes
	E-mail	Yes
	Password	Yes
	Department	Yes
	Role	Yes
	Affiliation	No
	Publications	No

	Awarded grants	No
	Default search settings	No
	Deadline notification preferences	No
	Saved Searches	No
	Tracked Opportunities	No
	Groups	No
	Researcher IDs (ex. ORCID)	No
	Keywords	No
	Expertise statement	No
	External Links	No
	Education	No
	Languages	No
	Associations	No
	Honors	No
	Photograph	No
	Publication Citations	No

	Awarded Grants	No
	Patents	No

6.1 - Data sharing

Information is not shared with any third party organizations or individuals.

6.2 - Data Flows

Data is collected and provided by library management (data controller) which provides library services for the patrons (data subjects) and imports this data into Pivot.

Pivot processing and data storage is performed in the United States (see Section 8.4). Ex Libris complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. Ex Libris has certified to the Department of Commerce that it adheres to the Privacy Shield Principles.

7 - Risks and Controls

Data processing involves high volume activities involving a large number of people or a larger percentage of the relevant population. The sensitivity of the information collected about individuals (patrons) is low. None of the data elements are considered special category (GDPR Article 9).

Specific risks and controls:

Main Risks	Key Controls
Disclosure of individuals' data to unauthorized party – internal users	- Access management controls, authentication and authorization mechanisms
Disclosure of individuals' data to unauthorized party – external party (e.g., hackers)	- Application security measures - Operational security including: data center security, server security and network security - Intrusion prevention - Contractual agreements - Security monitoring
Processing of personal data without proper need	- Contractual agreement - Privacy by Design processes managed by DPO, including privacy implementation in product development - Privacy assessments
Breach of individual rights	- Data Processing Agreement - Most individual rights are responsibility of data controller - Governance processes by DPO
The organization has not implemented a documented Privacy management framework	- Documented, published and implemented privacy policy - Appointed DPO, responsible for keeping the privacy processes current

8 - Privacy management framework

8.1 - GOVERNANCE

The development and implementation of the privacy framework is the responsibility of Ex Libris DPO, Ellen Amsel. This also includes involvement in product development and privacy processes implementation throughout Ex Libris.

8.2 - PRIVACY POLICY

 The privacy policy is clear and published in: https://www.proquest.com/about/Privacy-Home.html.

8.3 - SECURITY

The Information Security Policy is clear and published in:
https://knowledge.exlibrisgroup.com/Cross_Product/Security/Policies/Ex_Libris_Information_Security_Policy_v1.3.

Security controls include:

- Physical security
- Operational security
- Network security
- Intrusion prevention
- Application security
- Access control
- Asset management
- Backup controls
- Privacy management
- Risk management and compliance

8.4 - THIRD PARTY

Pivot is located in AWS and the ProQuest data center located in Virginia. Security controls regarding AWS are managed using their SOC2 (Type 2) audit report.

Personal data is not shared with any third parties.

8.5 - USER RIGHTS

Data is collected and provided by library management - data is processed according to the data processing agreement, and individual consent is the responsibility of the library (the data controller).

Ex Libris provides their customers with processes and tools to allow patrons the ability to access and correct their personal data and to delete their personal information in accordance with the library's policies. This is performed by library staff, using the Pivot interface. Any patron wishing to make a comment or complaint regarding their own information can contact the Ex Libris DPO.

8.6 - CONSENT

Consent is managed by the customer (library), who is the data controller.

8.7 - TRAINING & AWARENESS

Ex Libris is managing a privacy awareness training program, as well as a security awareness training program. Additionally, specialized Privacy by Design training has been conducted specifically for GDPR.

8.8 - INCIDENT HANDLING

Ex Libris has constructed incident response and notification procedures. Procedures include breach notification policy and the involvement of the DPO in case of a data breach. The process is tested at least once a year.

8.9 - PRIVACY BY DESIGN

Ex Libris has implemented Privacy by Design processes, which involve the DPO and privacy concerns from the beginning of product development and through change management.

8.9.1 - Data minimization

The information collected by Pivot (specific data elements listed above) is limited to the information necessary, relevant and proportionate to the purposes of the system use. Only personal data which is necessary for the processing is collected.

8.9.2 - Data retention

Data is never deleted from Pivot unless an individual asks to erase the information.

Pivot provides libraries with the ability to delete historical data when no longer needed so that they may implement their own data retention policies.