Ex Libris

Esploro Privacy Impact Assessment

Version 1.1

August 2020

Record of Changes

Date	Version	Author	Description of Change
December 2019	1.0	KPMG/Ellen Amsel	Creation
August 2020	1.1	KPMG/Ellen Amsel	Updated and reviewed

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 Esploro 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 Esploro and the privacy and security controls designed to mitigate those risks.

Since Esploro is part of the Higher-Ed platform (formerly known as the Alma platform), all security and privacy controls are provided by the security and privacy design of the Higher-Ed platform (please refer to the *Alma Privacy Impact Assessment*).

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.

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

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 the Esploro service, where Ex Libris is the data processor. The purpose for data processing is to manage and disseminate research output and data, leveraging library expertise

and technology, and seamlessly integrating with existing research workflows for Ex Libris customers.

It should be noted that Esploro is part of the Higher-Ed platform (formerly known as the Alma platform) and most If not all security and privacy capabilities are based on the same capabilities built into the Higher-Ed platform (please refer to the *Alma Privacy Impact Assessment*).

6 - Data Elements

Data needed for processing – information about the data subjects (researchers) are provided by the Ex Libris customer (institution authority), with assistance from Ex Libris with populating certain data fields. Additional personal data updates are done by the institution staff or the researchers themselves when needed, and the processes involved are the sole responsibility of the institution, which is the data controller. We note that personal data of librarians and other administrators of Esploro is processed by the Higher-Ed platform, formerly known as the Alma platform (please refer to the *Alma Privacy Impact Assessment*).

Following is a list of data elements related to the data subject (researcher), processed by Esploro. Some of the data elements are encrypted in the database. All of the data elements are related to the researcher.

Category	Data field	Mandatory
General Information	First Name	Yes
	Middle Name	No
	Last Name	Yes
	Name Suffix	No
	ID	No
	Full Address	No
	Phone	No

	E-mail	Yes

	Title	No
	Position	No
	Identifiers	No
	Researcher Record Type	Yes
	Languages	No
	Profile Picture	No
	Current Organization Affiliations	No
	Previous Organization Affiliations	No
	Research Topics and Keywords	No
	Area of Interest	No
	Researcher Website URLs	No
	Education	No
	Associations	No
	Honors	No

	Attachment	No
	Assets	No
	Grants	No

6.1 - Data sharing

Information is not shared by Ex Libris with any third party organizations or individuals. The Ex Libris customer determines how and what information is shared with third parties.

Notice about information collection and sharing is detailed in:
https://www.exlibrisgroup.com/privacy-policy-2/

6.2 - Data Flows

Data is collected and provided by institution management (data controller), which provides library and/or research services for the researcher (data subjects) and import this data into Esploro.

Data is not transferred by Ex Libris to any third party, except as authorized or initiated by the Ex Libris customer.

7 - Risks and Controls

Data processing involves high volume activities involving a large number of people or a larger percentage of the relevant population. Yet, the sensitivity of the information collected about individuals (researchers) 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

Ex Libris privacy policy, relating to Esploro, is published in: https://www.exlibrisgroup.com/privacy-policy-2/ and managed by the DPO.

8.3 - SECURITY

Information security policy is clear and published in: https://knowledge.exlibrisgroup.com/Alma/Product_Documentation/010Alma_Online_Help_(English)/010Getting_Started/020Security_and_Data_Privacy.

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

Ex Libris uses data center co-location providers. Ex Libris owns and manages all the equipment in the data center and monitors the security controls over the data center vendor using SOC2 (Type 2) audit reports. Additional information can be found at the Ex Libris Trust Center.

Personal data is not shared by Ex Libris with any third parties, except as authorized or initiated by the Ex Libris customer.

8.5 - USER RIGHTS

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

Ex Libris provides their customers with processes and tools to allow researchers 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 the library staff or research administrators, using the Esploro interface. Any researcher wishing to make a comment or complaint regarding their own information can contact the Ex Libris DPO.

8.6 - CONSENT

If, and to the extent required, consent is managed by the customer institution - the data controller.

8.7 - TRAINING & AWARENESS

Ex Libris is managing a privacy awareness training program for its personnel, 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.

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 Esploro (specific data elements listed above) is limited to the information determined by the Ex Libris customer as necessary, relevant and proportionate to the purposes of the system use. Only personal data determined as necessary by the Ex Libris customer is processed.

8.9.2 - Data retention

Esploro allows retention of historical data in order to support auditing needs. To reduce privacy risks, the system anonymizes certain historical data.

Esploro allows libraries or research administrators to delete historical data when it is not needed, allowing customers to implement their own data retention policies.

Unless Customer or the relevant individual objects, following termination of the Esploro subscription, Ex Libris intends to retain the institution researcher Profiles for use in cross-institution databases available to Ex Libris customers and/or public users.