Ex Libris

Rosetta Privacy Impact Assessment

December 2020

1 - Table of Contents

2 - Disclaimer

This report is provided to Ex Libris. If this report is received by anyone other than Ex Libris. The recipient is placed on notice that the attached report has been prepared solely for use in connection with Ex Libris, 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. and KPMG Somekh Chaikin. KPMG Somekh Chaikin shall have no liability for the use of this report by anyone other than Ex Libris. and shall pursue all available legal and equitable remedies against recipient, for the unauthorized use or distribution of this report.

3 - Purpose

The Privacy Impact Assessment (PIA) is a process that identifies what impact a project, product, service, 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 Ex Libris' Rosetta solution, the privacy impact of these processes, 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 Ex Libris' Rosetta solution, and the privacy and security controls designed to mitigate those risks.

Ex Libris' Rosetta solution is a software provided to customers as a standalone system without a connection to Ex Libris' infrastructure.

Ex Libris doesn't have access to any data stored in a customer's system, except when providing support to the customer. Any potential risk in these support processes is mitigated by Ex Libris' policy (8.2) and infrastructure.

5 - Scope and Plan

This PIA scope is Ex Libris' Rosetta solution.

In general, Ex Libris has no access to customers' data since it provides Rosetta as an on premise installation. We identified that during support processes for Rosetta an Ex Libris' support engineer may be exposed to customer's data which in this case makes Ex Libris a data processor.

This assessment doesn't include Ex Libris' SaaS solutions and Ex Libris' hosting of customers' on-premise installations.

6 - Data Elements

Ex Libris' exposure to data elements in an on premise installation of its customers is minimal and limited to support sessions when a remote connection to a customer's network is executed.

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-1-2/

As stated, the only scenario when an Ex Libris' employee may be exposed to customer information, which may include personal information, is during a support session. In this scenario Ex Libris' employee can't perform any action on the personal information including sharing it with others. This is a result of a policy (see 8.2) that prohibits copying any information from customer network to Ex Libris' network, and a network topology that physically separates the support infrastructure from Ex Libris' infrastructure.

6.2 - Data Flows

Same as 6.1

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

Ex Libris' risk as a result of an on premise Rosetta installation is very low. Even in cases that an Ex Libris' employee may be exposed to personal information it is limited in time and the information doesn't reside on Ex Libris' network or infrastructure.

Table 1 details the risks and the key controls that mitigate these risks.

Main Risks	Key Controls
Disclosure of individuals' data to unauthorized party – internal users	- Separation of environments between the remote connection infrastructure and Ex Libris' network. - A policy (see 8.2) prohibits the copying of customer information

Disclosure of individuals' data to unauthorized party – external party (like hackers)	- N/A since no customer information reside on Ex Libris' infrastructure.
Processing of personal data without proper need	- Separation of environments between the remote connection infrastructure and Ex Libris' network. - A policy (see 8.2) prohibits the copying of customer information
Breach of individual rights	- N/A since no customer information reside on Ex Libris' infrastructure.

8 - Privacy Management Framework

8.1 - Governance

Ex Libris is ISO 27701 (privacy information management system) certified. Adherence to the framework is the responsibility of Ex Libris DPO, Ellen Amsel. This includes the product development lifecycle and privacy processes implemented throughout Ex Libris.

8.2 - Remote Access to Customer Data (Support)

It is Ex Libris' policy not to copy customer's data and especially credentials in Salesforce and to contact customers personally if personal data is required to handle customer cases (for example, if the data is corrupted). Ex Libris asks its customers to send personal data using any channel that the customer considers secure by their institution security and privacy standards.

Additionally, Support works with test user accounts that are created specifically for replication and debugging purposes.

8.3 - Security

Ex Libris has implemented a multi-tiered security model that covers all technological aspects of the company. The security model and controls are based on international standards, such as ISO/IEC 27001:2005 and ISO/IEC 27002, the standards for an information security management system (ISMS). The full list of Ex Libris ISO certifications can be found here.

Information security policies are published in:
https://knowledge.exlibrisgroup.com/Cross_Product/Security/Policies

Security policies include:

- Cloud Security and Privacy
- Customer Appropriate Usage Statement
- Ex Libris Certified Third-Party Software and Security Patch Release Notes
- Ex Libris Cloud Services BCP
- Ex Libris New Third Party Software Evaluation and Plan
- Ex Libris Password Policy
- Ex Libris Security Incident Response Policy
- Ex-Libris Security Patches and Vulnerability Assessments Policy
- Welcome to the Ex Libris Cloud

8.4 - Third Party

There is no use of 3rd parties for support services.

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

Ex Libris is considered a data processor for any data that a support engineer may be exposed to even though Ex Libris, in its support processes, doesn't store any personal information. Therefore the "User Rights" article isn't relevant for Rosetta on premise implementation.

8.6 - Consent and Data Subject Rights

User consent, and other data subject rights, are managed by the data controller, therefore, it is the customer's responsibility to only allow access to the system for users who have expressed their consent for the relevant data processing.

8.7 - Training & Awareness

Ex Libris is managing a privacy awareness training, as well as security awareness training. The awareness training included GDPR specific training, which included Privacy by Design training.

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.

9 - Record of Changes

Type of Information	Document Data
Document Title:	Rosetta Privacy Impact Assessment
Document Owner:	Tomer Shemesh – Ex Libris Chief Information Security Officer (CISO)
Approved by:	Ellen Amsel, Privacy and Regulation Officer & DPO
Release date:	Oct 16 ,2018
Reviewed & Revised:	Tomer Shemesh

9.1 - Revision Control

Version Number	Nature of Change	Date Approved
1.0	Initial version	Oct 16 ,2018

2.0	Reviewed and updated	March 15, 2020
2.1	Reviewed and updated	October 22, 2020
2.2	Reviewed and updated	December 24, 2020