Ex Libris

Rosetta Privacy Impact Assessment

March 2018

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 of this document

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 the 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 the Ex Libris Rosetta product, and the privacy and security controls designed to mitigate those risks.

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

Ex Libris does not 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 Rosetta, an Ex Libris solution.

Because Rosetta is provided to the customer as an on premise solution, Ex Libris does not have access to customer data. We noted that during support processes for Rosetta, an Ex Libris support engineer may be exposed to customer data, which makes Ex Libris a data processor.

This assessment does not include the hosting of Rosetta at Ex Libris data centers.

6 - Data Elements

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

6.1 - Data sharing

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

6.2 - Data Flows

Same as 6.1

7 - Risks and Controls

Ex Libris risk regarding an on premise Rosetta installation is very low. Even in cases where an Ex Libris employee may be exposed to personal information, that exposure is limited in time and the information does not reside on the 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 resides 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.
Lack of documented and implemented Privacy management framework	- Documented, published and implemented policy (see 8.2). - Appointed DPO (Ellen Amsel), 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 - REMOTE ACCESS TO CUSTOMER DATA (SUPPORT)

It is Ex Libris policy not to copy customer data, and especially credentials in Salesforce, and to contact customers directly if access to personal data is required to resolve a customer case (for example, if the data is corrupt). Ex Libris asks its customers to send personal data using any channel that the customer considers secure by their institution, based on the institution's 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, including ISO/IEC 27001:2005 and ISO/IEC 27002, the standards for an information security management system (ISMS).

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 third parties for support services.

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, does not store any personal information. Therefore, the GDPR "User Rights" article is not relevant for a 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 privacy training and security awareness training. The privacy training includes GDPR specific training, which includes Privacy by Design training.

8.8 - INCIDENT HANDLING

Ex Libris has developed and implemented incident response and notification procedures. Procedures include a 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 addresses privacy concerns from the beginning of product development and through change management.