# Ex Libris

## Aleph 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 Ex Libris Aleph 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 Aleph solution and the privacy and security controls designed to mitigate those risks.

Ex Libris Aleph solution is provided to customers as a standalone system that has no connectivity 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 during a support process is mitigated by Ex Libris policy (8.2) and infrastructure.

## 5 - Scope and Plan

This PIA scope is Ex Libris Aleph solution.

Ex Libris does not have access to customer data because Aleph is installed on premise at the customer site. We noted that during support processes for Aleph, when Ex Libris connects to the customer's Aleph installation, an Ex Libris support engineer could potentially access customer data, at which point Ex Libris becomes a data processor.

This assessment does not include instances where Aleph is hosted at the Ex Libris data center.

## 6 - Data Elements

Ex Libris' exposure to customer data in an on premise installation is minimal and limited to support sessions when a remotely connecting to a customer's Aleph installation.

### *6.1 - Data sharing*

As noted above, only when Ex Libris provides support to the customer remotely, the Ex Libris engineer may potentially access customer information, which may include personal information. In accordance with Ex Libris policy, an Ex Libris engineer may not 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 engineers from copying any information from the customer system to Ex Libris and a network topology that physically separates the support infrastructure from Ex Libris infrastructure. Should a customer wish Ex Libris to work with their information, the customer must send their data to Ex Libris securely based on the customer's security policies.

### *6.2 - Data Flows*

See 6.1

## 7 - Risks and Controls

Because Alep is on-premise at the customer location, the risk to customer data from Ex Libris is very low. Even in cases where an Ex Libris may be exposed to personal information it is limited in time and the information does not 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 customer on-premise installation of Aleph and the Ex Libris network<br>- 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 customer data does not reside on the Ex Libris infrastructure |
| **Processing of personal data without proper need** | - Separation of environments between the remote connection infrastructure and Ex Libris network<br>- A policy (see 8.2) prohibits the copying of customer information |
| **Breach of individual rights** | - N/A since no customer information resides on the Ex Libris infrastructure |
| **Lack of documented and implemented Privacy management framework** | - Documented, published and implemented policy (see 8.2)<br>- 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'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). We ask our customers to send us personal data using any channel that the customer considers secure by their 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 3rd parties

## 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 "User Rights" are the responsibility of the data controller for Aleph on premise implementations.

## 8.6 - CONSENT

User consent is 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 training, as well as security awareness training. The privacy training incorporates GDPR specific training, including Privacy by Design training.

## 8.8 - INCIDENT HANDLING

Ex Libris has developed and implemented 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 addressing privacy concerns from the beginning of product development and through change management.

### 8.9.1 - Data minimization

There is an ongoing process for data minimization by policy (see 8.2) and by infrastructure topology.

Due to these limitations, no personal information is collected by Ex Libris

### 8.9.2 - Data retention

Data retention rules are the responsibility of the data controllers, and should be defined by Ex Libris customers.