



Ex Libris

Aleph Privacy Impact Assessment

March 2020



1 - Table of Contents

1 - Table of Contents	2
2 - Disclaimer	2
3 - Purpose of this document.....	4
4 - Main findings and Conclusions.....	4
5 - Scope and Plan	5
6 - Data Elements	5
6.1 - Data sharing.....	5
6.2 - Data Flows	5
7 - Risks and Controls.....	6
8 - Privacy management framework	7
8.1 - GOVERNANCE	7
8.2 - PRIVACY POLICY	7
8.3 - SECURITY	7
8.4 - THIRD PARTY.....	7
8.5 - USER RIGHTS	7
8.6 - CONSENT	8
8.7 - TRAINING & AWARENESS	8
8.8 - INCIDENT HANDLING	8
8.9 - PRIVACY BY DESIGN	8

2 - Disclaimer



This report is provided to Ex Libris Ltd. If this report is received by anyone other than 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 ALEPH 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 ALEPH platform 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.

Individuals' personal data in ALEPH is limited in nature and the inherent risks resulting is not high. The privacy controls designed and implemented comply with GDPR requirements, relating to the business processes of ALEPH.

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.

5 - Scope and Plan

This PIA scope is the ALEPH service, where Ex Libris is the data processor. The purpose for data processing is to manage print, electronic, and digital materials in a single interface 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 subjects (patron & staff), processed by ALEPH.

Patron:

Patron ID, Name (first, last), Address, E-mail, Zip Code, Telephone, SMS Number, Receive SMS Status, Proxies/Sponsor, Salutation, Title, Date of Birth, Gender, Place of Birth.

Staff:

User (ID), Password, Name, Email, Address, Telephone

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 the customers (data controller), which provide library services for the patrons (data subjects), and import this data into ALEPH.

Administrator server access is subject to a change management process and is authorized and monitored using CyberArk, a privileged account management solution.

Data is not transferred to any third party or to other countries.

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 (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	<ul style="list-style-type: none"> - Access management controls, authentication and authorization mechanisms
Disclosure of individuals' data to unauthorized party - external party (e.g., hackers)	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - Contractual agreement - Privacy by Design processes, managed by DPO, including privacy implementation in product development - Privacy assessments - Change management process - PAM solution
Breach of individual rights	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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 ALEPH, is published in: [https://knowledge.ExLibrisgroup.com/Cross_Product/Security/Policies/Cloud Security and Privacy Statement](https://knowledge.ExLibrisgroup.com/Cross_Product/Security/Policies/Cloud_Security_and_Privacy_Statement) and managed by the DPO.

8.3 - SECURITY

Information security policy is clear and published in:

[https://knowledge.ExLibrisgroup.com/Cross_Product/Security/Policies/Cloud Security and Privacy Statement](https://knowledge.ExLibrisgroup.com/Cross_Product/Security/Policies/Cloud_Security_and_Privacy_Statement)

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 one vendor for ALEPH - Equinix co-location provider. Ex Libris owns and manages all the equipment in the data center and monitors the security controls over this vendor, using 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 individuals' 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 the library staff, using the ALEPH 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 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 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

The information collected by ALEPH (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

ALEPH allows retention of historical data. The customer is in full control of the data stored in the service and has responsibility to determine the retention requirements for the customer's data. On a regular basis, Ex Libris performs system backups of application



files, database files, and storage files. The privacy controls in practice at Ex Libris are enforced for all backup files. All backup files are retained for 10 weeks.

ALEPH allows libraries to delete historical data, when this is not needed, in order to implement their own data retention policies.