### Table of Contents

1 - Table of Contents ......................................................................................................................... 2  
2 - Disclaimer .......................................................................................................................................... 3  
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 ................................................................................................................................... 6  
   6.2 - Data Flows ..................................................................................................................................... 6  
7 - Risks and Controls ............................................................................................................................... 6  
8 - Privacy management framework ......................................................................................................... 7  
   8.1 - GOVERNANCE .............................................................................................................................. 7  
   8.2 - SECURITY ...................................................................................................................................... 7  
   8.3 - THIRD PARTY ............................................................................................................................... 8  
   8.4 - USER RIGHTS ............................................................................................................................. 8  
   8.5 - TRAINING & AWARENESS .......................................................................................................... 8  
   8.6 - INCIDENT HANDLING ............................................................................................................... 8  
   8.7 - PRIVACY BY DESIGN ............................................................................................................... 9  
9 - Record of Changes ............................................................................................................................... 10  
   9.1 - Revision Control ......................................................................................................................... 10  

© 2020 KPMG Somekh Chaikin, an Israeli member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.
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, 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 Primo system, the privacy impact of this, 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 Primo system, and the privacy and security controls designed to mitigate those risks. Primo implementation can be stand-alone or part of an Alma implementation. In cases where it is part of an Alma implementation, much of the user management is done by Alma, and GDPR compliance issues relating thereto are covered in 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 customer), such as consent management.

Primo – Research and Discovery SaaS solution, allows researchers and library users (patrons) to explore, access and share library resources, along with the library management system. In some cases, system functionality is limited to specific institutional users, such as university employees. In these cases, user identification is required and is done by the institution systems.

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 start and maintaining this while products and services are developing. In order to keep compliance, Ex Libris will have to continue putting privacy of its clients and end-users as a core value, and lead by example for other SaaS vendors in the market.
5 - Scope and Plan

The PIA scope is Primo, where Ex Libris is the data processor. The purpose of data processing in Primo is to provide a library discovery service that seamlessly integrates with a wide range of library and academic systems for end-to-end efficient workflows.

Some Primo functionality (such as search) can be used anonymously, but other functionality (such as saving to favorites and placing requests) is limited to authenticated institutional users only and will require login.

Primo implementation can be part of an Alma implementation. In these cases, users are primarily managed by Alma, and GDPR compliance issues are covered in the Alma Privacy Impact Assessment.

End user patrons are generally authenticated by the institution’s authentication system while Primo system administrators are authenticated by Primo (or by Alma for Primo implemented with Alma).

6 - Data Elements

Data needed for processing – information about the data subjects (typically, library staff and patrons) are provided by the Ex Libris customer. Additional personal data updates are done by the library staff and patrons 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 subject, processed by Primo.

<table>
<thead>
<tr>
<th>Patron/Staff Member</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Email</td>
</tr>
<tr>
<td></td>
<td>Home Address</td>
</tr>
<tr>
<td></td>
<td>Mobile number</td>
</tr>
<tr>
<td></td>
<td>User ID</td>
</tr>
</tbody>
</table>
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://exlibrisgroup.com/privacy-policy-1-2/

6.2 - Data Flows

Data is collected and provided by the library management (data controller), which provides library services for the patron (data subjects) and imports this data into Primo.

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 many people or a larger percentage of the relevant population. Yet, the sensitivity of the information collected about individuals is low. None of the data elements are considered special category (GDPR Article 9).

Specific risks and controls:

<table>
<thead>
<tr>
<th>Main Risks</th>
<th>Key Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disclosure of individuals’ data to unauthorized party – internal users</td>
<td>- Access management controls, authentication and authorization mechanisms</td>
</tr>
</tbody>
</table>
| 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 |

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 - SECURITY

Ex Libris has implemented a multi-tiered security model that covers all aspects of our cloud-based systems. 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).


Security controls include:

- Physical security
- Operational security
- Network security

© 2020 KPMG Somekh Chaikin, an Israeli member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.
- Intrusion prevention
- Application security
- Access control
- Asset management
- Backup controls
- Privacy management
- Risk management and compliance

8.3 - 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.

8.4 - 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 its customers with processes and tools to access and correct data subject personal data, and to delete the personal information in accordance with the library’s policies. This is performed by the library staff. Any patron wishing to make a comment or complaint regarding their own information can contact the Ex Libris DPO.

8.5 - TRAINING & AWARENESS

Ex Libris conducts privacy training and security awareness training for its personnel. The Privacy training includes extensive Privacy by Design training for relevant personnel.

8.6 - 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.
Ex Libris has implemented Privacy by Design processes that involve the DPO and addressing privacy concerns from the beginning of product development and throughout the product lifecycle.
9 - Record of Changes

<table>
<thead>
<tr>
<th>Type of Information</th>
<th>Document Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Title:</td>
<td>Primo Privacy Impact Assessment</td>
</tr>
<tr>
<td>Document Owner:</td>
<td>Tomer Shemesh – Ex Libris Chief Information Security Officer (CISO)</td>
</tr>
<tr>
<td>Approved by:</td>
<td>Ellen Amsel, Privacy and Regulation Officer &amp; DPO</td>
</tr>
<tr>
<td>Release date:</td>
<td>Oct 16, 2018</td>
</tr>
<tr>
<td>Reviewed &amp; Revised:</td>
<td>Tomer Shemesh</td>
</tr>
</tbody>
</table>

9.1 - Revision Control

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Nature of Change</th>
<th>Date Approved</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial version</td>
<td>Oct 16, 2018</td>
</tr>
<tr>
<td>2.0</td>
<td>Reviewed and updated</td>
<td>March 15, 2020</td>
</tr>
<tr>
<td>2.1</td>
<td>Section 8.3 updated</td>
<td>August 25, 2020</td>
</tr>
<tr>
<td>2.2</td>
<td>Reviewed and updated</td>
<td>November 16, 2020</td>
</tr>
<tr>
<td>2.3</td>
<td>Reviewed and updated</td>
<td>January 31, 2021</td>
</tr>
</tbody>
</table>