Ex Libris

Summon Privacy Impact Assessment

March 2018

1 - Table of Contents

2 - Disclaimer

This report is provided to ExLibris Ltd. If this report is received by anyone other ExLibris Ltd. The recipient is placed on notice that the attached report has been prepared solely for use in connection with ExLibris Ltd. and this report and its contents may not be shared with or disclosed to anyone by the recipient without the express consent of ExLibris Ltd. and KPMG Somekh Chaikin. KPMG Somekh Chaikin shall have no liability for the use of this report by anyone other than ExLibris 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 Summon system, the privacy impact of this, and the measures ExLibris is taking in order to manage the risks involved.

4 - Main Findings and Conclusions

We have reviewed the privacy risks regarding Summon system, and the privacy and security controls designed to mitigate those risks.

Summon – Research and Discovery System, is allowing researchers explore, access and share library resources, along with the library management system.

It should be noted that Summon system does not require user identification, and does not process personalinformation.

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. Personal information is not processed by Summon.

Summon implementation can be part of an Alma implementation. In these cases, since user management is part of the system, GDPR compliance issues must be considered – and are covered in the Alma Privacy Impact Assessment.

After reviewing all material GDPR aspects, our impression is that there are no privacy related risks in Summon. Ex Libris efforts in implementing GDPR requirements are well managed, resulting in a good level of compliance.

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, ExLibris 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

Summon is a resource discovery solution that does not require user identification. The system does not process personal information.

In some cases, system functionality is limited to users who are some institution members, such as university employees. In these cases, user identification is required and done by the institution systems. Personal information is not processed by Summon.

Summon implementation can be part of an Alma implementation. In these cases, since user management is part of the system, GDPR compliance issues must be considered – and are covered in the Alma Privacy Impact Assessment.

In other cases, user identification is done by library's single sign-on system. In those cases, the library is responsible for privacy issues.

6 - Data Elements

Summon data elements are focused in indexing and discovery of library resources and do not include patron (library user) identifiable information.

Resource discovery data is not associated with user identification.

6.1 - Data sharing

Information in the system is owned by the university and not shared with any external party.

6.2 - Data Flows

Data is collected in cataloging and indexing processes, while the content is from a large variety of content providers. The data elements are not associated with specific individuals.

7 - Risks and Controls

Since no personal information is involved, there are no privacy risks.

8 - Privacy management framework

8.1 - GOVERNANCE

The development and implementation of the privacy framework is the responsibility of the ExLibris DPO, Ellen Amsel. This includes involvement in the product development lifecycle and privacy processes implemented throughout ExLibris.

In cases of systems that do not process personal information, it is the responsibility of the DPO to ensure that future system changes will not involve personal data in system processes or databases, or ensure that any new privacy risks introduced in the future will be handled properly.

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).

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

Security policies include:

- Cloud Security and Privacy Statement
- 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

8.3 - THIRD PARTY

ExLibris uses one vendor for Summon – Equinix co-location, that provides the physical housing and physical security for the data center. ExLibris manages the security controls over this vendor, using SOC2 (Type 2) audit report.

Personal data is not shared with any third party.

8.4 - USER RIGHTS

Summon system does not process any personal information, therefore data subject rights are not relevant to Summon.

Use cases that involve user identification, through Alma, are covered in the Alma Privacy Impact Analysis.

Use cases that involve other library single sign-on systems are the responsibility of the institution.

8.5 - TRAINING & AWARENESS

ExLibris is managing privacy training and security awareness training. The Privacy training includes extensive Privacy by Design training.

8.6 - INCIDENT HANDLING

ExLibris 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.

8.7 - PRIVACY BY DESIGN

ExLibris 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.