KPMG

Exlibris Ltd

Leganto 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 Leganto 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 Leganto system, and the privacy and security controls designed to mitigate those risks.

Leganto - Reading Lists Management System allows instructors to create reading lists for students, and gives the students an integrated solution, along with the library management system.

It should be noted that the user-management functionality in Leganto relies on Alma, and therefore individuals' related information is based on the combination of the two systems. Resulting, most of the GDPR related requirements are fulfilled in Alma.

ExLibris is a data processor of the data, with the universities as the data controllers. Subsequently, many of the responsibilities around data subject rights are the universities'.

Individuals' personal data in Leganto is limited in nature and the inherent risks resulting is low. The privacy controls are designed and implemented in order to comply with GDPR requirements, relating to the business processes of Leganto.

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.

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

This PIA scope is the Leganto application – ExLibris is a data processor of the data. The Institution, which is the Ex Libris customer, determines the purposes and means of the processing of personal data, and therefore is the data controller.

The purpose for data processing is to provide Institutions (instructors and students) with solution specialized interface for reading lists, including reading lists development, instructor and student notes, collections, and usage analysis.

Leganto is integrated with Alma, and relies on Alma's database for user, and other resources, management.

6 - Data Elements

Leganto runs on the Alma platform; users must be registered in Alma in order to access Leganto.

Data Privacy Risks of Alma are detailed a separate report - Alma Privacy Impact Assessment report, and are not the scope of this report.

The data elements in Leganto include reading lists and notes, both of instructors and students. This information can be associated with an individual only through the Alma database, which contains the user identity.

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 the following processes:

- Reading lists creation and management by instructors and librarians.
- Reading lists notes and usage from students.

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

7 - Risks and Controls

Data processing involves high volume activities, yet the information in the system does not contain individuals' data – this information is managed in Alma. Following, the sensitivity of the information collected is low.

Specific risks and controls:

Main Risks	Key Controls
Disclosure of individuals' data to unauthorized party - internal users	- Individuals' information is manage in Alma, and the privacy and security controls regarding this information pertain to Alma (see: Alma DPIA).
Disclosure of individuals' data to unauthorized party - external party (like hackers)	
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 clearly defining customer responsibilities as a controller - Most individual rights are responsibility of data controller - Governance processes by DPO
The organization has not implemented a documented Privacy management framework	- 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 the ExLibris DPO, Ellen Amsel. This includes involvement in the product development lifecycle and privacy processes implemented throughout ExLibris .

8.2 - PRIVACY POLICY

Ex Libris privacy policy relating to Leganto, is published in: LINK.

8.3 - 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

8.4 - THIRD PARTY

ExLibris uses one vendor for Leganto – 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.

8.5 - USER RIGHTS

User rights are managed by the Institution through the Institution's identity and access management system, which is integrated into Alma. Leganto access is controlled through Alma.

ExLibris is a processor for Leganto data. User access rights are of the responsibility of the Institution, which is the data controller (customer).

Data processing agreements with customers (intitutions) clearly define that, with regard to the processing of personal data, the customer is the Controller, and Ex Libris is the Processor.

Execution of data subject rights is the responsibility of the Institution using Leganto's interface. Because user identification and authentication is performed through Alma, some of the data subject rights must be performed in Alma, not Leganto (for example, data rectification by university authorized staff).

8.6 - CONSENT

User consent is managed by the data controller, therefore, it is the Institution's responsibility to ensure that only users who have provided their consent for the relevant data processing be allowed access to Leganto.

8.7 - TRAINING & AWARENESS

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

8.8 - 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.

8.9 - 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 through change management.

8.9.1 - Data minimization and Data retention

Data minimization is performed in Alma, which is the platform for Leganto.

The information collected by Leganto (specific data elements listed above) is limited to the information necessary, relevant and proportionate to the purposes of the system use.