Ex Libris

360 Services Privacy Impact Assessment

April 2018

1 - Table of Contents

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 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 360 Services, the privacy impact, and the measures Ex Libris is taking in order to manage the risks identified.

4 - Scope and Plan

The name “360 Services” refers to a suite of software products including 360 Core (Client Center), 360 Resource Manager, 360 Consortium Edition, 360 MARC Updates, 360 Link, E-Journal Portal, 360 Counter, 360 Search, Intota, and Intota Assessment. The only products that store personal data are 360 Core and Intota and are the scope of this PIA. Both products will be referred in after as "360 Services." Ex Libris is the data processor in 360 Services. The purpose for data processing is to manage print, electronic, and digital materials in a single interface for Ex Libris customers.

5 - Main Findings and Conclusions

We have reviewed the privacy risks regarding 360 Services and the privacy and security controls designed to mitigate those risks.

It should be noted that for 360 Services, 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.

Personal data in 360 Services is limited in nature and the inherent risks resulting is low. The privacy controls designed and implemented comply with GDPR requirements, relating to the business processes of 360 Services.

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 throughout the product lifecycle.

6 - Data Elements

Data needed for processing – In 360 Services, information about the data subjects (library contacts and staff users) 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 (contacts & staff), required for processing by 360 Services.

Contact:

Last name

Staff:

First name, Last name, email address

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), whose staff users (data subject) manage library resources. Staff users enter this staff user data into 360 Services, and may optionally enter contact (data subject) information into 360 Services.

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. The sensitivity of the information collected about individuals (staff users and contacts) 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	- Access management controls, authentication and authorization mechanisms
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 - Change management process - PAM solution
Breach of individual rights	- 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	- 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

ProQuest privacy policy relating to 360 Services is published in: https://www.proquest.com/go/privacy 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

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 360 Services – Equinix co-location provider that provides the physical housing and physical security for the data center. 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 consent is the responsibility of the library (the data controller).

Ex Libris provides their customers with processes and tools to allow staff users 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 360 Services interface. Any staff user 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 throughout the product lifecycle including change management process.

8.9.1 - Data minimization

The information collected by 360 Services (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 processing is collected.

8.9.2 - Data retention

360 Services allows retention of historical data. The customer is in full control of the data stored and is responsible for determining the retention requirements for the customer's data.

360 Services allows libraries to delete historical data when not needed in order to implement their own data retention policies.