Ex Libris

campusM Privacy Impact Assessment

February 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 campusM 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 campusM SaaS services and mobile application, and the privacy and security controls designed to mitigate those risks.

campusM is a mobile application, allowing staff, students and university candidates personalized access to university services and information.

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 campusM 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 campusM.

After reviewing all material GDPR aspects, the privacy risks and implemented controls, any residual risk that we found was minimal. Our impression is that ExLibris efforts in implementing GDPR requirements are well managed, and after further implementation of some of the open tasks, will result in 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 the start, and maintaining this while products and services are developing. In order to maintain compliance, ExLibris will need to continue putting the 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 campusM application – ExLibris is a data processor of the data. Ex Libris' customers, the universities, determine the purposes and means of the processing of personal data, and therefore, are the data controllers.

The purpose for data processing is serving Universities, students, university candidates and alumni with mobile and web SaaS services for many in-campus services, including university information and alerts, class attendance and other integrated services (using system APIs) such as grades and library management.

6 - Data Elements

Data needed for processing – in most cases, data is entered into the system by end-users, or collected from the mobile app. Only data that is needed for system functionality is stored.

It should be noted that the mobile application is presenting a vast variety of information from integrated data sources. This information is not stored in the system, but rather presented directly from the data source API to the mobile app.

Following is a list of data elements related to individuals, processed by the system:

Data Category	Description and Data Fields
User data	This is general end user information and identification details. *Fields include: First name, last name, email address, username.*
Device Data	This data enables the platform to send alerts and notifications and identify service call source. *Fields include: Device Identifier, platform, model.*
Roles Data	This data consists of roles that can be applied to end users to personalize their experience. *Fields include: role name, role description.*

Alerts Data	This is the data that is used to send messages, as well as the content sent. *Fields include: notification title, content, device identifier.*
Insight Data	This is analytical data used to inform customers of app usage. *Fields include, hit type, hit description, URL, device data, IP address.*
App Manager Data	This includes general app administrator details to enable access. *Fields include: First name, last name, email address, App Manager* *Username, App Manager password*
In-App Feedback	This data is provided by the end user in regard to their app experience and is available for review within App Manager *Fields can include: Page title from where feedback was given, feedback text.*
Attendance Data	Optional component used to capture student attendance. *Fields include: email, event information, beacon location, check-in type, IP address.*
Directory Data	This is for data that can optionally be made available to enable students to browse or search for colleagues and staff on campus. *Fields can include: First name, last name, email address, office location, contact details, email.*

6.1 - Data sharing

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

6.2 - Data Flows

The data in campusM comes from two sources: the University and the mobile app users – while a user registers to the app, the user is entering basic personal data.

Some university services require authentication with university directory services – this authentication is done directly with the university infrastructure, and this authentication data is not stored in campusM servers (some cache is stored in the mobile app, but not in the backend systems).

The mobile app is collecting device information and application usage data (insights). This information allow analytical reports, which are shared with the university staff.

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

6.3 - Legacy engagements data

campusM was developed by oMbiel, which was acquired by ExLibris. Past campusM engagements lead to processing and storage of data that is no longer needed by current system clients, including precise location data, user photos and other data. ExLibris is taking steps for deletion of data which is no longer required, and the efforts for GDPR compliance include the completion of this task. Removal of unnecessary data is planned to be completed by April 2018.

7 - Risks and Controls

Data processing involves high volume activities involving a large number of people or a larger percentage of the relevant population.

campusM is collecting class attendance data, however, this data is not precise location data, and this information is only available while the student's timetable requires class attendance. Therefore, the information collected does not disclose a user location, besides actual attendance in a class, which is in the student's timetable.

The system does not collect data elements that 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
Breach of individual rights	- Data Processing Agreement clearly defining customer responsibilities as the data 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
Handling data elements from past system engagements are not in compliance with GDPR requirements	- Historical data and legacy implementations data deletion process

8 - Privacy management framework

8.1 - GOVERNANCE

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

8.2 - PRIVACY POLICY

campusM privacy policy is referenced in the EULA (End-User License Agreement), published in the campusM website and managed by the DPO. It is also published on the campusM website.

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 campusM – Equinix hosting provider. ExLibris manages 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

ExLibris is a processor for the campusM data. Responsibilities for most user rights are of the data controllers, which are the universities, Ex Libris' customers.

Data processing agreements with customers (universities) clearly define, acknowledge, and agree 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 might be dependent on processes that Ex Libris should perform on behalf of its customers. In order to allow data access, rectification, erasure, and data portability, user requests are made through the user's university, and the university either processes the request or forwards the request for Ex Libris to handle on the customer's behalf.

Users wishing to exercise his or her privacy rights, to obtain additional information, or to make a comment or complaint regarding the privacy policy or its implementation, can also contact the Ex Libris Privacy Officer.

8.6 - CONSENT

User consent is managed by the data controller, therefore, it is the university responsibility to only allow access to the system to users who have expressed their consent for the relevant data processing.

8.7 - TRAINING & AWARENESS

Ex Libris is managing a privacy training, as well as security awareness training. The training includes GDPR specific Privacy by Design training.

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

There is an ongoing process for data minimization of campusM by the DPO and product team. This process includes deletion of data from past customer engagements that is no longer necessary for the current purpose of data processing.

The information collected by campusM (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

Data retention rules are the responsibility of the data controllers and should be defined by Ex Libris customers – the execution of data retention processes is performed by Ex Libris upon request from its customers.