



# Ex Libris

## SFX (Hosted) Privacy Impact Assessment

April 2018



## 1 - Table of Contents

1 - Table of Contents .....	2
2 - Disclaimer .....	2
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.....	5
6.2 - Data Flows .....	5
7 - Risks and Controls.....	5
8 - Privacy management framework .....	6
8.1 - GOVERNANCE .....	6
8.2 - PRIVACY POLICY .....	6
8.3 - SECURITY .....	6
8.4 - THIRD PARTY.....	7
8.5 - USER RIGHTS.....	7
8.6 - CONSENT .....	7
8.7 - TRAINING & AWARENESS.....	7
8.8 - INCIDENT HANDLING.....	8
8.9 - PRIVACY BY DESIGN .....	8

## 2 - Disclaimer

© 2018 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.



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 Ltd. and KPMG Somekh Chaikin. KPMG Somekh Chaikin shall have no liability for the use of this report by anyone other than Ex Libris 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 the SFX (Hosted) service, the privacy impact, 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 SFX (Hosted) platform and the privacy and security controls designed to mitigate those risks.

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 customers), such as consent management.

Individuals' personal data in SFX (Hosted) 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 SFX (Hosted).

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 while products and services are developing. In order to maintain compliance, Ex Libris will need to continue their practice of making the privacy of its customers a core value, and lead by example for other SaaS vendors in the market.

## 5 - Scope and Plan

This PIA scope is the SFX (Hosted) service, where Ex Libris is the data processor. The purpose for data processing is to manage print, electronic, and digital materials in a single interface for Ex Libris customers.

## 6 - Data Elements

SFX does not store any specific information about a patron other than the IP address, and possibly institution, Faculty and user group are defined by the library. This data is stored in the statistics tables in order to allow the library to process statistics queries by these parameters.

### 6.1 - Data sharing

Information is not shared with any third party organizations or individuals.

### 6.2 - Data Flows

Data is kept scrambled in the statistics tables and cannot be read directly by someone with access to the server.

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

The sensitivity of the information collected about individuals (patrons) 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	<ul style="list-style-type: none"> <li>- Access management controls, authentication and authorization mechanisms</li> </ul>
Disclosure of individuals' data to unauthorized party - external party (e.g., hackers)	<ul style="list-style-type: none"> <li>- Application security measures</li> <li>- Operational security including: data center security, server security and network security</li> <li>- Intrusion prevention</li> </ul>

	<ul style="list-style-type: none"> <li>- Contractual agreements</li> <li>- Security monitoring</li> </ul>
<b>Processing of personal data without proper need</b>	<ul style="list-style-type: none"> <li>- Contractual agreement</li> <li>- Privacy by Design processes, managed by DPO, including privacy implementation in product development</li> <li>- Privacy assessments</li> <li>- Change management process</li> <li>- PAM solution.</li> </ul>
<b>Breach of individual rights</b>	<ul style="list-style-type: none"> <li>- Data Processing Agreement</li> <li>- Most individual rights are responsibility of data controller</li> <li>- Governance processes by DPO</li> </ul>
<b>The organization has not implemented a documented Privacy management framework</b>	<ul style="list-style-type: none"> <li>- Documented, published and implemented privacy policy</li> <li>- Appointed DPO, responsible for keeping the privacy processes current</li> </ul>

## 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

Ex Libris privacy policy, relating to SFX (Hosted), is published in:

[https://knowledge.exlibrisgroup.com/Cross\\_Product/Security/Policies/Cloud\\_Security\\_and\\_Privacy\\_Statement](https://knowledge.exlibrisgroup.com/Cross_Product/Security/Policies/Cloud_Security_and_Privacy_Statement) 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](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 SFX (Hosted) - 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 individuals' consent is the responsibility of the customer (the data controller).

Ex Libris provides their customers with processes and tools to allow patrons 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 SFX (Hosted) interface. Any patron 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 through change management.

---

### 8.9.1 - Data minimization

The information collected by SFX (Hosted) (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 the processing is collected.

---

### 8.9.2 - Data retention

SFX (Hosted) allows libraries to delete historical data, when no longer needed, in order to comply with their own data retention policies.