
Cloud Security and Privacy Statement_2.2

Version 2.2

A newer version is available [here](#)

Security

This section describes the Ex Libris security procedures.

Introduction

Ex Libris, a ProQuest company, is committed to providing its customers with a highly secure and reliable environment for our hosted and cloud-based applications. We have therefore developed a multi-tiered security model that covers all aspects of hosted and cloud-based Ex Libris systems. The security model and controls are based on international protocols and standards and industry best practices, including ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2014, ISO/IEC 22301:2012, ISO/IEC 27701:2019 and CSA Star Self-Assessment.

Ex Libris has received several security and privacy certifications, including ISO/IEC 27001:2013, ISO/IEC 27018:2014, ISO/IEC 27017:2015, ISO/IEC 22301:2012, ISO/IEC 27701:2019 and CSA Star Self-Assessment. The ISO/IEC 27018:2014 standard establishes commonly accepted control objectives, including controls and guidelines for protecting Personally Identifiable Information (PII) for the public cloud computing environment in accordance with the privacy principles in ISO/IEC 29100. ISO/IEC 27017:2015 provides a code of practice for information security controls, including guidelines that expand upon the ISO/IEC 27002 standard by adding security controls specifically related to cloud computing. The ISO/IEC 22301:2012 standard focuses exclusively on business continuity management (BCM). The ISO/IEC 27701:2019 provides guidance for establishing, implementing, maintaining and continually improving a privacy information management system (PIMS). The CSA Star Self-Assessment provides transparency and quality assurance for Ex Libris cloud services.

The ISO/IEC 27001:2013 standard provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS).

The ISO certification business processes scope are the Development processes, cloud services, global support services, professional services, operational services, library management services, learning & research solutions. The scope service is for all Ex Libris cloud based services.

As part of the company's focus on security issues, Ex Libris employs a Privacy and Regulation Officer & DPO, a Chief Information Security Officer (CISO), and a dedicated Cloud Services team with responsibility for:

- Applying the security model to all system tiers
- Monitoring and analyzing the infrastructure for suspicious activities and potential threats
- Issuing periodic security reports to Ex Libris management and customers
- Dynamically updating the security model and addressing new security threats
- In addition, the Ex Libris Security team is dedicated to:
 - Systematically examining the organization's information security risks, taking into account threats and vulnerabilities
 - Designing and implementing a coherent and comprehensive suite of information security controls and/or other forms of

risk treatment (such as risk avoidance or risk transfer) to address the risks that are deemed unacceptable

- Adopting an overarching management process to ensure that the information security controls continue to meet the organization's evolving information security needs

Physical Security Protocols

Security controls at Ex Libris data centers are based on standard technologies and follow the industry's best practices. The physical security controls are constructed in such a way as to eliminate the effect of single points of failure and retain the resilience of the computing center.

SSAE16 SOC1

The Ex Libris data centers have a SSAE16 SOC1 service auditor's report as the result of an in-depth audit of the centers' control objectives and control activities, including controls over information technology and all other related processes.

Environmental Controls

A variety of environmental controls are implemented at the Ex Libris data center facilities.

- Servers are locked inside the infrastructure in a designated area.
- The server area is cooled by a separate air conditioning system, which keeps the climate at the desired temperature to prevent service outage.
- The facilities are protected by a fire suppression system, which protects the computing equipment and has built-in fire, water, and smoke detectors.
- The facilities have on-site generators, which serve as an alternative power source.
- There is 24-hour video surveillance of all entrances and exits, lobbies, and ancillary rooms. The videos are recorded and monitored, and be retained for later use.

Physical Access Control

Physical access to the data center is restricted to personnel with a business need to access the infrastructure. All physical access activities are logged and monitored. All visitors need to be approved beforehand, and the approval is for a limited period of time. Visitors must be accompanied by an authorized employee throughout their visit.

Operational and Information Security Protocols

Operating System

Operating systems used in the cloud are hardened according to best practices in the industry. Only services and components that are necessary to support the application stack are activated; the administrator user always has a password set up, and only necessary ports in the firewall are open.

Network Security

Firewalls: Applications in the hosting and cloud have firewalls installed to shield them from attack and prevent the loss of valuable customer data. The firewalls are configured to serve as perimeter firewalls to block ports and protocols.

Network-Based Intrusion Detection and Prevention

The combination of an intrusion detection system (IDS) and intrusion prevention system (IPS) installed and tracks all illegal activities. The system sends real-time alerts and proactively blocks communication once a suspicious attack is discovered. The system performs various activities on the network: log collection and analysis from the various machines (firewalls, switches, and routers), file integrity checking, and rootkit detection.

Data Elimination

Ex Libris has strict procedures and a unique policy for handling obsolete data based on the DoD 5220.22-M standard. These procedures are also applied if a customer decides to stop using our software. Disks and tapes are destroyed once they are no longer needed. Tapes are overwritten with the next use. CDs that are no longer needed are destroyed by a CD/DVD data crusher or shredder. All storage devices that may need to be used again are cleaned by data wipe software.

Backup

On a regular basis, Ex Libris performs system backups to back up application files, database files, and storage files. All backup files are subject to the privacy controls in practice at Ex Libris. The restore procedures are tested on an ongoing basis to ensure rapid restoration in case of data loss.

Application Security

Development Life Cycle and Maintenance

Ex Libris implements a number of practices to keep each stage of the software development life cycle secure. These include:

- Planning – During the planning stage, the Ex Libris Chief Information Security Officer (CISO) submits a report specifying the product's security requirements. The report includes the security requirements covering all of the solution components, such as the application, the database, and the client side. To manage security issues optimally, the Ex Libris Chief Information Security Officer (CISO) uses various methods, such as access control, auditing, and monitoring.
- Design and Development – The Ex Libris Chief Information Security Officer (CISO) verifies that the design and development of the product are based on our security guidelines. Other security issues are addressed by an additional security-gap requirements document. The security code review is tested on security-sensitive parts of the application.
- Implementation, Testing, and Documentation – Unit, integration, and system testing confirm that security requirements are properly implemented. The requirements are documented and become standard policy.
- Deployment and Maintenance – The Ex Libris Chief Information Security Officer (CISO) is responsible for identifying, managing, and minimizing security vulnerabilities. The Ex Libris Chief Information Security Officer (CISO) also performs quarterly penetration tests or security reviews.

Access Control

The following items are relevant for access control:

- Access control – Access to the infrastructure is limited, based on role and responsibility and is only available to Operations and Professional Services for maintaining and supporting customers.
- Authentication – Ex Libris also enforces a strict role based password policy that applies to both layers - the operational team members and the application's users. Passwords are stored in an encrypted form, using a one-way encryption method based on an industry-standard hash algorithm. Only the application is able to compare the hashed and entered passwords. In some cases Ex Libris grants the customer full root access and full control. Customers can implement

their own password based on their password policy (depending on products, service level, and their contract agreement).

- Authorization and Privacy – Multi-tenancy and shared resources are basic characteristics of the Hosting and SaaS architecture. Resources, such as storage, and networks are shared between users. Data privacy and protection may be compromised, as the European Network and Security Agency explains, if there is “a failure of mechanisms separating storage, memory, routing, and even reputation between different tenants of the shared infrastructure” (<http://www.enisa.europa.eu/media/faq...0Computing.pdf>). Therefore, strict data isolation is applied in the application to all layers of the application. Data isolation will be defined based on either shared resources using firewall rules for network isolation, Oracle VPD, or separate databases for database isolation and separate files and permissions for files sharing isolation.

Since the privacy and confidentiality of its customers' data are the company's top priority, Ex Libris has developed extended authorization controls and additional security processes to protect customer privacy. The authorization mechanism in Ex Libris applications supports the segregation of duties. Segregation of duties is applied in order to minimize the risks and the possibility of misusing privileges.

Ex Libris has instituted the following policies in order to protect customer data:

- Customer data is protected with Oracle technologies.
- Personal information is protected.
- Sensitive personal information such as bank information and credit cards are not stored by Ex Libris.

Customer data, including private data, is deleted based on the Data Elimination section on page 6, and backed up customer data is deleted periodically.

All access control activities produce logs with enough information to meet auditing requirements and support usage charges. In addition, access control activities generate notifications to designated users to prevent users from setting up rogue accounts or otherwise modifying access entitlements.

Asset Management

The following items are relevant for asset management:

- Incident Management – NIST defines a computer security incident as “a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.” (<http://www.csirt.org/publications/sp800-61.pdf>). To handle security incidents effectively, Ex Libris has constructed incident response and notification procedures.
- Ex Libris employs a dedicated Incident Handling team that responds to security incidents and mitigates risks. The team uses monitoring and tracking tools and performs real-time analysis. Additionally, the team has clear procedures in place for communicating the incidents to any involved party and for handling escalations. Every incident is forwarded to the Ex Libris Chief Information Security Officer (CISO) for assessment and analysis.
- Personnel Security – Ex Libris realizes that the malicious activities of an insider could have an impact on the confidentiality, integrity, and availability of all types of data and has therefore formulated policies and procedures concerning the hiring of IT administrators or others with system access. Ex Libris has also formulated policies and procedures for the ongoing periodic evaluation of IT administrators or others with system access. User permissions are continuously updated and adjusted so that when a user's job no longer involves infrastructure management, the user's console access rights are immediately revoked.
- Background Checks – Once a candidate has been offered a job with Ex Libris and before he or she begins employment, we conduct a background check. For all background checks and reference checks we receive a release from the candidate prior to starting the screening process. We use a third party to conduct our background checks. The standard check includes S.C check, criminal history, employment verification, and reference checks. Any additional checks are conducted based on business needs.

Regulatory Compliance

SSAE16 SOC1 – As described earlier, Ex Libris data facilities went through an in-depth audit of their control objectives and control activities and a SSAE16 SOC1 audit report was issued.

Ex Libris Privacy Policy

About This Policy

This Privacy Policy describes the privacy practices of Ex Libris Ltd. and Ex Libris (USA) Inc. and their respective subsidiary companies, including Ex Libris (Deutschland) GmbH, Ex Libris (UK) Limited, Ex Libris (France) SARL, Ex Libris Italy S.R.L., Ex Libris (Scandinavia) A/S, Ex Libris (Australia) Pty. Ltd. and Ex Libris Asia Pacific PTE. LTD. (collectively, “Ex Libris”, “we,” “our,” or “us”) with respect to how we collect, use, store, disclose and transfer the information (a) you provide when you interact with us through our websites and when you communicate with us through other means such as email or by telephone, and (b) provided by your institution and you, for its (and your) use of our services and applications, such as Alma, Primo, Leganto, campusM, Aleph Hosted, Voyager Hosted and most of our other cloud-based services (the “Ex Libris Services”) – please see below under Ex Libris Services-Customer Data.

This Privacy Policy governs websites owned or operated by Ex Libris that provide a link to this Privacy Policy on the homepage of the site (“**Ex Libris Sites**”).

Ex Libris (USA) Inc. is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

Data Controller or Data Processor

Ex Libris is the data controller for data described by this policy except as specified below, which means that Ex Libris determines the purposes and means of the processing of personal data.

Ex Libris is the data processor with respect to personal data submitted to and stored on the Ex Libris Services for hosting and processing purposes as further described below under Ex Libris Services-Customer Data.

Types of Information We Collect About You

Information you or your Institution may provide

Depending upon the Ex Libris Sites you are accessing or other method of contact, we may collect information such as

- Contact details such as (for example) your full (i.e., first and last) name, institutional affiliations, phone number, email address, and postal address
- Educational and professional background information
- Usernames and passwords that may be used on some of the Ex Libris Sites
- Comments, feedback, posts and other content you submit to the Ex Libris Sites
- Information you provide to or post on message boards or chat rooms that are part of the Ex Libris Sites
- Interests and communication preferences.

Where we are collecting directly (and not being provided the information by your institution), you will be given advanced notice of what information specific to you we are collecting. Posting information on message boards or in chat rooms is never required.

Information collected automatically

As you navigate the Ex Libris Sites, Ex Libris may also automatically collect information about you or your computer or device that does not directly identify you. This information may include IP address and device identifiers, information about your Internet connection and information about the equipment or software you use to access the Ex Libris Sites. Such information is only collected to the extent that it is necessary for us to provide services that you use, to optimize your user experience, and/or to make improvements to the Ex Libris Sites and service offerings. Ex Libris does not serve third party advertising.

You have the ability to choose to opt out of inclusion of your personal information at the point of disclosure. You may choose whether your personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by you. You may also opt out of use of your personal information as outlined below under Access, Correction, and Erasure.

How We Collect Information About You

We collect information about you in three main ways:

- **Information Directly Provided by You or Your Institution:** We collect information about you when you register for services, download an app, sign up for email or text alerts, request products or services, respond to surveys, fill out registration forms on an Ex Libris Site or otherwise for events, register for or view webinars; create a profile, publicly post or share content, contact us, use social media connections, and/or otherwise interact with Ex Libris Sites. We may receive and store information provided by your institution to the extent required to perform a contracted service.
- **Information Collected Automatically Using Technological Means:** As described above under Information Collected Automatically, we collect certain information automatically using technological means. We also use cookies as further described below under Cookies and Similar Technologies. You may set your browser to block all cookies, including cookies associated with Ex Libris Sites, or to indicate when a cookie is being set by us. However, it is important to remember that certain services may not function properly (or at all) if your cookies are disabled. Please see our Cookies and Tracking Information page (<http://www.exlibrisgroup.com/cookie-policy>) for more information about how we use cookies.
- **Information Collected Through Third Parties:** We may receive information about you from customers and business partners for referral and reference purposes.

Cookies and Similar Technologies

Ex Libris uses cookies to manage and improve the functionality of our websites and to enable us to better understand how you use our services. A cookie is a tiny text document, which usually includes anonymous information about the user. Unless specifically noted on our Cookies and Tracking Information page (<http://www.exlibrisgroup.com/cookie-policy>), our cookies are not used to serve advertising and we do not provide any usage or search data to advertising agencies. You can set your browser to not accept Ex Libris' cookies, but you might not be able to access all aspects of the Ex Libris Site you are visiting.

How We Use and Share Information About You

Ex Libris uses the information we collect to perform the services requested, for the purposes of authorizing and processing transactions, authenticating users, customer service, customer support, content processing, content classification, and providing you with information concerning Ex Libris services. We will retain this information for as long as the customer account is active or as needed to provide the Ex Libris services, comply with our legal obligations, resolve disputes, and as needed to comply with or enforce our licenses and other agreements.

To be clear, we do not access or use Customer Data (as defined below) processed through the Ex Libris Services except

for the purposes set forth in our agreement with the relevant customer. Please see below under Ex Libris Services-Customer Data.

Ex Libris remains responsible for the personal data that we share with third parties for processing on our behalf, and we remain liable under this privacy policy if such third parties process such personal data in a manner inconsistent with this privacy policy and we are responsible for the event giving rise to the damage.

Please keep in mind that any information you disclose publicly – either in a public profile or through message boards or other public areas – may be collected and used by others, may be indexable by search engines, and might not be able to be erased from public view to the extent they have been copied to external sites. Please be careful when disclosing personal information in these public areas.

The following is a list of instances where we may share your information with third parties:

- **Institutions or Businesses.** If you access a service through your affiliation with an institution or through your employer, your information and certain usage data gathered through the Ex Libris service may be shared with the institution or business for the purposes of usage analysis, access and license management, collection management, contract and regulatory compliance, and cost allocation.
- **Publishers/Content Providers:** We may provide anonymized information to publishers so that they understand how their content is being used and consumed.
- **Service Providers.** At times Ex Libris may hire other companies to process data or do work on our behalf. This is always pursuant to a contract that requires the third-party service provider to protect your information consistent with this privacy policy. These companies are only provided the information they need to perform their functions and the information can only be used to perform the services on our behalf or to comply with legal requirements. We do not disclose personal information to third parties for direct marketing purposes.
- **Message Boards and Other Public Areas:** Information you post on message boards, chat rooms, or other public areas that are part of the Ex Libris Sites is public and will not be kept private. Should you wish to remove your postings from message boards or other public areas, follow the instructions under the **Access, Correction, and Erasure** section of this policy.
- **Affiliates:** To facilitate Ex Libris' global operations, Ex Libris may share and transfer information we collect with its affiliates located in countries around the world. For example, Ex Libris may need to share such information with other companies within the Ex Libris corporate family for customer support, marketing, technical operations and account management purposes.
- **Contests and Sweepstakes:** We may publicly disclose the name, city and state of contest and sweepstakes winners as permitted by the contest/sweepstakes rules or as required by law. You may be required to consent to such disclosure if you wish to enter a given contest or sweepstakes.
- **Sale or Purchase of Business or Assets:** If Ex Libris is involved in a merger, acquisition, or asset sale, we will continue to ensure the confidentiality of any personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.
- **Legal Reasons:** We will disclose information to cooperate with law enforcement, government or regulatory bodies, content protection organizations, or judicial processes as required by the applicable laws and regulations. We may also use or disclose information to enforce or protect the rights or safety of Ex Libris Services users, us, or others. We will provide notice to individuals prior to such disclosures, to the extent it is practicable to do so and allowed by law.

Security

Ex Libris takes commercially reasonable security measures to protect against unauthorized access to, or unauthorized alteration, disclosure or destruction of, data that you share and that we collect and store. These security measures may include practices such as keeping your data on a secured server behind a firewall, internal reviews of our data collection practices and platforms, industry-standard encryption technologies, and physical security measures to guard against unauthorized access to systems where we store your information.

If you have reason to believe that a third-party has gained unauthorized access to your information, please contact us

immediately at privacy@exlibrisgroup.com. If Ex Libris becomes aware of any data breach, we will notify affected individuals or, with respect to Ex Libris Services, affected institutions as soon as reasonably possible.

Your Rights and Choices

Communication Preferences and Opt-outs

If you have subscribed to one or more of our email newsletters or are receiving marketing emails from us and you don't want them anymore, you can unsubscribe. Follow the instructions contained in the email message to opt-out of receiving future messages of that type. However, you cannot unsubscribe from some service related messages so long as you maintain an account with Ex Libris.

Access, Correction, and Erasure

Postings from message boards or other public areas, may be deleted by using the tools provided when you are logged-in to the particular service; or you may contact Ex Libris at privacy@exlibrisgroup.com with the details and location of the content (such as a direct link to the information), and Ex Libris will make commercially reasonable efforts to remove the content.

You may request to review, correct or delete the personal information that you have previously provided to us through the Ex Libris Sites. For requests to access, correct or delete your personal information, please send your request along with any details you may have regarding the method by which the information was submitted to privacy@exlibrisgroup.com. Requests to access, change, or delete your information will be addressed within a reasonable timeframe.

To help protect your privacy and security, we will take reasonable steps to verify your identity, such as requiring a password, user ID, or other verification before granting access to or removing your information.

Please note that where we are acting as a processor of personal data for our customer, we may first refer your request to the customer that submitted your personal data, and we will assist our customer as needed in responding to your request, as further described below under Ex Libris Services-Customer Data.

Please contact privacy@exlibrisgroup.com for more information about exercising these rights.

Data Retention and Deletion

If you request to delete your personal information, we will endeavor to fulfill your request but some personal information may persist in backup copies for a certain period of time and may be retained as necessary for legitimate business purposes or to comply with our legal obligations.

Ex Libris may retain your information for a period of time consistent with the original purpose of collection, and for a reasonable time thereafter in accordance with applicable law. We also may retain your information during the period of time needed for Ex Libris to conduct audits, comply with our legal obligations, resolve disputes and enforce our agreements.

Children

The Ex Libris Sites are typically general audience websites, intended for use by users aged 13 and older.

We do not market to nor intentionally collect any personally identifiable information from children under thirteen (13) years of age. If you are under 13, please do not register for any of our services or Sites or provide us with any personally identifying information (such as your name, email address or phone number). Please contact privacy@exlibrisgroup.com if you are aware of any personal information supplied to one of Ex Libris Sites by a child under the age of thirteen (13).

Links to Other Services and Websites

The Ex Libris Sites may contain links to information created and/or maintained on third-party websites. The third-party website will be displayed in a new browser window and the user will no longer be in the Ex Libris environment. When users select a link to an outside website, they are leaving the Ex Libris Site and are subject to the privacy and security policies of the owners of the third-party website. We are not responsible for, and we do not endorse or control, the policies or practices of any such website or services.

In some cases, we may embed a content feed, video player or other application from a third party into the Ex Libris Site, and those feeds, players, or other applications may appear to be part of the Ex Libris Site, even though they are provided or served by a third party. Such feeds, video players, and/or applications do not collect personal information from you. If information is required for the performance of the service, the service provider is required to protect your information consistent with this privacy policy. For further information, please see the “How We Share Information About You” section of this policy.

Ex Libris Services – Customer Data

Ex Libris customers submit data and information to the Ex Libris Services for hosting and processing purposes (“Customer Data”). Our customers are data controllers with respect to Customer Data and Ex Libris is a data processor. The Ex Libris Services include cloud-based library management, discovery, research and reading list solutions, mobile/web platforms for students and other institutional end users and other software as a service or hosted solutions and related services specified in our agreements with such customers. While Ex Libris’ customers decide what Customer Data to submit to the Ex Libris Services, depending on the particular service, the Customer Data submitted regarding its students, faculty, staff, library patrons, suppliers, users and other individuals may typically include contact details such as name, role, phone number, email address, institutional identification number and postal address, information regarding library and research activity, mobile/web platform information exchange and messaging, and information collected automatically described in this privacy policy.

Ex Libris will not use or share any such Customer Data except as provided in its agreements with such customers, or as may be required by law. In accordance with such agreements, Ex Libris may access, transfer and process Customer Data only for the purpose of providing the Ex Libris Services, preventing or addressing service or technical problems or other purposes as set forth in such agreements or required by law. Additional information about the Company’s privacy and security practices with respect to Customer Data is available on our website, currently at https://knowledge.exlibrisgroup.com/Cross_Product/Security .

Ex Libris acknowledges that you have the right to access, correct, amend and delete your personal information. If personal information pertaining to you as an individual has been submitted to us by an Ex Libris customer and you wish to exercise any rights you may have to access, correct, amend, or delete such data, please inquire with our customer directly. Because Ex Libris is subject to our agreements with customers (as the data controller) with respect to your personal information stored on the Ex Libris Services, if you wish to make your request directly to Ex Libris, please provide the name of the Ex Libris customer who submitted your data to the Ex Libris Services. We will refer your request to that customer, and will support the customer as needed in responding to your request within a reasonable time frame.

Updates to Our Privacy Policy

From time to time, we may revise this Privacy Policy. If we make material revisions to the way we collect or use your information, we will provide you with notice of those changes by either: (1) notifying you directly, (2) announcing the change on the Ex Libris Sites, and/or (3) posting the revised version of this Privacy Policy online.

You can determine when this Privacy Policy was last revised by referring to the “Last Updated” legend at the top of this

page. By continuing to use Ex Libris Sites after such updates, you affirm your agreement with the terms of the Privacy Policy. If we have made changes you don't agree with, you are free to request that we delete your information as set out in the Your Rights and Choices section above.

Questions

For any questions on this Privacy Policy or our data practices, you can contact us at privacy@exlibrisgroup.com.

Despite the measures outlined in this Privacy Policy, Ex Libris cannot guarantee the security of any information that is disclosed online. To the extent permissible under law, Ex Libris shall not be liable for any direct, indirect, special, incidental, consequential or punitive damages relating to this Privacy Policy.

EU-US and Swiss-US Privacy Shield Frameworks

Ex Libris (USA) Inc. complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States, respectively. Ex Libris (USA) Inc. has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern.

To learn more about the Privacy Shield program, and to view our certification, please visit <https://www.privacyshield.gov/>. Personal data from the European Union or Switzerland and/or on EU or Swiss citizens may be collected by Ex Libris and may be stored and processed in the United States or any other country in which Ex Libris or its affiliates, subsidiaries or agents maintain facilities.

You have the right to access your personal data, and to have the data corrected, amended or deleted where it is inaccurate or processed in violation of the Privacy Shield Principles.

Dispute Resolution

In compliance with the EU-US Privacy Shield Principles and the Swiss-US Privacy Shield Principles, Ex Libris commits to resolve complaints about your privacy and our collection or use of your personal information.

Step 1: Contact Ex Libris.

If you have an inquiry or complaint regarding whether Ex Libris has violated its obligations under this Privacy Policy as to you or if you are an EU or Swiss resident with an inquiry or complaint regarding whether Ex Libris has violated its obligations under the Privacy Shield Principles as to you (your "Complaint"), you should first contact Ex Libris' Global Privacy and Regulation Officer & DPO.

By mail to:

Ex Libris (USA) Inc.
Attn: Ellen Amsel, Privacy and Regulation Officer & DPO
1350 East Touhy Avenue
Des Plaines, IL 60018
USA

By email at: privacy@exlibrisgroup.com

Ex Libris will acknowledge your Complaint within 24 hours, and respond to your complaint within 45 days. Ex Libris may

ask that you provide additional information and/or request a one-on-one discussion or conference.

Step 2: Third Party Dispute Resolution.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider, TRUSTe, (free of charge) at <https://feedback-form.truste.com/watchdog/request>.

If you have a complaint left unresolved by all available recourse mechanisms, you may invoke binding arbitration. For additional information go here: www.privacyshield.gov/article?id=How-to-Submit-a-Complaint

Ex Libris has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved Privacy Shield complaints concerning data transferred from the EU and Switzerland.

Record of Changes

Type of Information	Document Data
Document Title:	Cloud Security and Privacy Statement
Document Owner:	Tomer Shemesh - Ex Libris Chief Information Security Officer (CISO).
Approved by:	Eyal Alkalay – Ex Libris Sr. Director of Cloud Engineering
Issued:	Apr 18, 2012
Reviewed & Revised:	Jan 03, 2019

Revision Control

Version Number	Nature of Change	Date Approved
1.0	Initial version	Apr 18, 2012
1.1	Updated – Tomer S	Apr 22, 2013

Version Number	Nature of Change	Date Approved
1.2	Review and Update- Tomer S	May 20, 2014
1.3	Review and Update- Tomer S	May 1, 2015
1.4	Review and Update- Tomer S	Apr 11, 2016
1.5	Review and Update- Tomer S	Jun 5, 2017
2.0	Review and Update- Tomer S	Apr 26, 2018
2.1	Review and Update- Tomer S	Aug 28, 2018
2.2	Review and Update - Tomer S	Jan 03, 2019

Document Distribution and Review

The document owner will distribute this document to all approvers when it is first created and as changes or updates are made. This document will be reviewed and updated annually or upon written request by an approver or stakeholder. Questions or feedback about this document can be directed to the owner or a listed approver