



What You Need to Know About Addressing GDPR Data Subject Rights in Alma

Version 1.3



Not Legal Advice

This document is provided for informational purposes only and must not be interpreted as legal advice or opinion. Customers are responsible for making their own independent legal assessment of the GDPR and their compliance obligations.

DISCLAIMER

The information in this document is subject to change and updating without prior notice at the sole discretion of Ex Libris. Please confirm that you have the most current documentation. There are no warranties of any kind, express or implied, provided in this documentation. This information is provided AS IS and Ex Libris shall not be liable for any damages for use of this document, including, without limitation, consequential, punitive, indirect or direct damages.

Any references in this document to third-party material (including third-party Web sites) are provided for convenience only and do not in any manner serve as an endorsement of that third-party material or those Web sites. The third-party materials are not part of the materials for this Ex Libris product and Ex Libris has no liability for such materials.

TRADEMARKS

"Ex Libris, Part of Clarivate" the Ex Libris bridge, Primo, Aleph, Alephino, Voyager, SFX, MetaLib, Verde, DigiTool, Preservation, URM, Voyager, ENCompass, Endeavor eZConnect, WebVoyage, Citation Server, LinkFinder and LinkFinder Plus, and other marks are trademarks or registered trademarks of Ex Libris Ltd. or its affiliates.

The absence of a name or logo in this list does not constitute a waiver of any and all intellectual property rights that Ex Libris Ltd. or its affiliates have established in any of its products, features, or service names or logos.

Trademarks of various third-party products, which may include the following, are referenced in this documentation. Ex Libris does not claim any rights in these trademarks. Use of these marks does not imply endorsement by Ex Libris of these third-party products, or endorsement by these third parties of Ex Libris products.

Copyright Ex Libris Limited, 2022. All rights reserved.

Web address: <http://www.exlibrisgroup.com>

Record of Changes

Date	Version	Author	Description of Change
January 15, 2020	1.0	Ellen Amsel	Creation
December 6, 2020	1.1	Ellen Amsel	Updated and reviewed
January 25, 2022	1.2	Itai Veltzman	Update Transaction Details
August 24, 2022	1.3	Daniel Friedman	Reviewed and updated

Table of Contents

Disclaimer	5
Introduction	5
Definitions	5
Summary of Data Subject Rights	7
Addressing GDPR Data Subject Rights with Alma	10
1. Rights of Data Subjects – Patrons.....	11
2. Rights of Data Subjects – Staff.....	15
1. Data Fields of User in Alma	20
2. Staff Audit Trial.....	31

Disclaimer

This paper is based on Ex Libris' understanding of certain requirements of the GDPR. However, the application of the requirements of the GDPR is highly fact specific, and many aspects and interpretations of GDPR are not well-settled.

As a result, this paper is provided for informational purposes only and should not be relied upon as legal advice or to determine how GDPR might apply to you and your organization. We encourage you to work with a qualified legal professional to discuss GDPR, how it applies specifically to your organization, and how best to ensure compliance.

Introduction

On May 25, 2018, a new privacy law called the General Data Protection Regulation (GDPR) took effect in the European Union (EU). It replaces the Data Protection Directive (Directive"), which had been in effect since 1995. While the GDPR preserves many of the principles established in the Directive, the GDPR gives individuals greater control over their personal data and imposes many new obligations on organizations that collect, handle, or process personal data.

Ex Libris is committed to GDPR compliance across all of our products and services. We have closely analyzed the requirements of the GDPR, and our engineering, product, security and legal teams have been working to align our procedures, documentation, contracts and services to support compliance with the GDPR. We also support our customers with their GDPR compliance journey with our strong foundation of certified security and privacy controls.

This paper describes tools and capabilities built into Alma that can assist your organization in addressing data subject rights and requests as a *controller* under the GDPR of personal data processed on Alma.

Definitions

Personal Data means any information relating to an identified or an identifiable natural person (**Data Subject**); an identifiable natural person is one who can be identified,

directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. With respect to the use of Alma, the customer is the **controller**.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. With respect to the use of Alma, Ex Libris is the **processor**.

Data Subject is an identified or an identifiable natural person to whom personal data relates (e.g., patrons and staff).

As you read through this paper, keep in mind that your compliance with the GDPR involves your role as the **controller** and Ex Libris as the **processor**.

Summary of Data Subject Rights

The rights of data subjects provided by the GDPR include the following:

1. *Right to be Informed (Article 13, 14 GDPR)*

The right to be informed encompasses your obligation to provide '*fair processing information*', typically through a privacy notice. It emphasizes the need for transparency over how you use personal data.

2. *Right of Access (Article 15 GDPR)*

Under the GDPR, individuals have the right to obtain:

- Confirmation that their data is being processed
- Access to their personal data; and
- Other categories of information - some of which should be provided by the controller in a privacy notice (see Article 15).

3. *Right to Rectification (Article 16 GDPR)*

Individuals are entitled to have their personal data rectified if it is inaccurate or incomplete without undue delay. If you have disclosed the personal data in question to third parties, you must inform such third parties of the rectification unless this proves impossible or involves disproportionate effort. You must also inform the individuals about the third parties to whom the data has been disclosed where requested.

4. *Right to Erasure (Article 17 GDPR)*

This right is also known as the *Right to be Forgotten*. It enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to have their personal data erased and to prevent further processing of their personal data in specific circumstances delineated in the GDPR, such as:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the processing was based on consent, and the individual has now withdrawn their consent.
- When the individual objects to processing and there are no overriding legitimate grounds for continuing the processing.
- The personal data was unlawfully processed.
- The personal data has to be erased in order to comply with a legal obligation in Union or Member State law to which the controller is subject.

There are circumstances described in the GDPR where the right to erasure may not apply and a controller can resist a request for erasure.

5. *Right to Restrict Processing (Article 18 GDPR)*

When this right is exercised you are permitted to store the personal data but not further process it. The *Right to Restrict Processing* applies in the specific circumstances set forth in the GDPR, including:

- Where an individual contests the accuracy of the personal data, then processing should be restricted for a period enabling the controller to verify the accuracy of the personal data.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If you no longer need the personal data but are required by the individual to establish, exercise or defend a legal claim.
- Where an individual has objected to processing for reasons specified in the GDPR, pending the verification whether the legitimate grounds of the controller override those of the individual.

6. *Right to Data Portability (Article 20 GDPR)*

This right allows individuals to receive the personal data the individual provided to a controller in a structured, commonly used and machine-readable format and to transmit such data to another controller, without hindrance from the original controller. In

exercising this right, the individual shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

The *Right to Data Portability* applies where the individual has given consent to the processing of their personal data for one or more specific purposes, or where processing is carried out by automated means or in other circumstances specified in the GDPR.

7. *Right to Object (Article 21 GDPR)*

Individuals have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data which is based on certain specified provisions of the GDPR, including profiling based on those provisions.

8. *Right Related to Automated Decision Making and Profiling (Article 22 GDPR)*

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the individual or similarly significantly affects the individual. The GDPR provides certain exceptions and conditions to this right.

9. *Right Related to Data Breach Notification (Article 34 GDPR)*

The GDPR introduces a duty on controllers to report certain types of data breaches to the relevant supervisory authority, and in some cases to the individuals affected by the breach.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Where a breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller is required to communicate the personal data breach to the data subjects without undue delay.

Addressing GDPR Data Subject Rights with Alma

The following section describes the capabilities of Alma that can assist customers in complying with the rights of data subjects. We have provided the information once for Patrons as the Data Subject and once for Staff users as the Data Subject.

1. Rights of Data Subjects – Patrons

Data Subject Right	Corresponding Alma Functionality
Right to be Informed	Ex Libris provides comprehensive documentation regarding Alma. Upon request, Ex Libris will provide you with additional relevant information you may need for addressing the Right to be Informed in relation to the processing of personal data by Alma.
Right to Access	<p>As Data Controller, you have full access to patron data in Alma at all times and can search for, export, and delete portions of that data that relate to an individual patron at any time.</p> <p>In Alma, a customer administrator manages the users and their information. The library can configure the fields that are typically used by most libraries such as, first name, last name, email address, and primary identifier.</p> <p>In the case of a patron's request to identify what categories of personal data are stored in Alma, the customer administrator will need to provide details on the data elements used by the customer in practice - Alma Analytics can be used to report on the user data elements to determine if they are used or not (e.g. if they are present in the data or null).</p> <p>Alma also allows the customer administrator to generate a copy of the patron's personal data undergoing processing by using the SIS Integration Profile's ability to extract a sample file for a specific user record. For more details see here (Look for 'Create Sample File').</p> <p>Examples of the information that may be loaded to Alma includes:</p> <ul style="list-style-type: none">• Picture – The Administrator can store user pictures on an external server and for display as part of the User Details page• General Information – such as job details, gender and birth date• Contact Information – Emails, phone numbers and addresses

	<ul style="list-style-type: none"> • Identifiers – Other than the primary identifier other identifiers can be associated with a user, such as a student ID, barcode, social login ID, and so forth. • Notes – There can be multiple notes gather for various elements in the system such as address, circulation, registration, etc. • Blocks – Added for users who have fines, outstanding loans, or repeated late book returns • Fines and fees – information on fines and fees waived on the user • Statistics – Additional statistical categories assigned to the user specifically to be used in Analytic reports • Attachments – All attachments added manually or sent automatically using the letter sending process. User letters sent by Alma are retained indefinitely and available on the attachments tab of the User Details. • Proxy – A proxy user can loan and return items on behalf of another user <p>For more details see section Data fields on User in Alma below.</p>
Right to Rectification	<p>A library staff user with the relevant privileges can edit and correct inaccurate personal data in Alma via existing standard functionality.</p>

Right to Erasure (Right to be Forgotten)

Alma offers the option to edit and delete (anonymize) user information.

[Deleting a User \(Patron\) from Alma](#)

The Alma user administrator or system administrator can delete a user.

To delete a user follow the instructions in the [Deleting Users](#). To delete a group of users, use the 'Purging Users job' as described in the Online Help, [Purging Users](#).

Users should be deleted in accordance with your Data Retention Policy. The information scope being deleted can be determined by the administrator in the following configuration: [Delete User Policy Settings](#)

Alma runs anonymization jobs on the following data elements:

- Loans
- Requests
- Resource Sharing Requests
- Fines & Fees

See more information about anonymization of personal information in the [Online Help](#).

Data that is anonymized in Alma is reportable in Analytics only in its anonymized format.

A user's data is also deleted (anonymized) from other parts of the system where the user data is not essential for ongoing Alma operations. This includes the deletion of a user's data from the user audit trail records based on the user audit retention period parameter. The parameter indicates the number of days for retaining the data.

See [User Audit History](#) for more information.

	<p>A weekly job, 'User audit purge with retention', deletes history records that are older than specified in the retention period. In addition a weekly job called "Letters Purge with Retention", deletes letters, if they created more than the configured number of days ago. See Setting Letter Retention Periods.</p> <p>Additional technical information can be found in the Ex Libris Developer Network: Patron Purge in Alma</p> <p>After the expiration or termination of the customer's Alma Subscription, Ex Libris will make available the customer data (including personal data), and delete existing copies unless legally prohibited. Unless otherwise agreed or required by applicable law, deletion of personal data from Alma and back-ups is generally completed within 90 days following final termination of the customer's Alma Subscription.</p>
Right to Restrict Processing	<p>Should a Data Subject wish to object to the processing of their personal data, the individual's Alma user record could be deleted. In addition, customers have the ability in Alma to provide shared/anonymous accounts to users who are entitled to restrict your processing of their data.</p>
Right to Data Portability	<p>Alma offers the ability to export personal data in standard formats using standard API export functionality. Please see here information about the "Get User Details" API</p>
Right to Object	<p>Alma provides you with the full ability to determine which Patrons to include in the data stored in Alma. Patrons that exercise their "right to object" could be excluded from the patron data load into Alma. Patrons may also be deleted as described above.</p>
Right related to Automated Decision Making and Profiling	<p>Any profiling or automated decision-making is determined and set by the customer. Generally, reports and task lists generated in Alma are designed to be used by humans for decision making.</p>

Right related to Data Breach Notification	<p>Ex Libris has procedures for data breach handling including notification. In the case of a personal data breach, Ex Libris will, as soon as possible and within 72 hours after having become aware of it, notify the customer.</p> <p>The notification will :</p> <ul style="list-style-type: none"> • Describe the nature of the personal data breach • Communicate the name and contact details of the data protection officer • Describe the likely consequences of the personal data breach • Describe the measures taken or proposed to be taken by Ex Libris <p>When required by the GDPR, the institution/library as Data Controller, is responsible for notifying the Supervisory Authorities and the affected data subjects.</p> <p>Ex Libris Security Incident Response Policy is available in the Ex Libris Knowledge Center - here</p>
--	---

2. Rights of Data Subjects – Staff

The following section describes the capabilities of Alma that can assist customers in complying with the rights of the data subjects with respect to its staff.

Data Subject Right	Corresponding Alma Functionality
Right to be Informed	<p>Ex Libris provides comprehensive documentation regarding Alma. Upon request, Ex Libris will provide you with additional relevant information you may need for addressing the Right to be Informed in relation to the processing of personal data by Alma.</p>

<p>Right to Access</p>	<p>The customer (institution) remains in control of its data. Ex Libris products enable customers to provide the required information to the data subject (patron or library personnel).</p> <p>The staff data stored is dependent on the roles and activities of the staff user:</p> <ul style="list-style-type: none"> • Personal information; For more details see section Data fields on User in Alma below • Audit on staff user activity in the system <p>User Information Card – In various places in Alma a staff User Information icon is displayed beside a user name. Clicking on the icon will display information about the user. An administrator can define the user information fields that are displayed in this pop-up box.</p> <p>Additional information can be found in Configuring User Information for Pop Ups</p> <p>Audit on staff activity in the system</p> <p>Alma stores audit information on staff activity in the system as part of functional and security needs. The information is kept using the user ID without any additional personal information. The audit trail can be seen based on staff permissions and system configuration. Additional technical information can be found in the Ex Libris Developer Network: User Management</p>
<p>Right to Rectification</p>	<p>A library staff user with the relevant privileges can edit and correct inaccurate personal data in Alma user administration via existing standard functionality.</p>

<p>Right to Erasure (Right to be Forgotten)</p>	<p>The Alma user administrator or system administrator can delete a staff user. In order to delete a staff user follow the instructions in Deleting Users.</p> <p>To delete a group of users, use the Purging Users job as describe in Purging Users. Users should be deleted in accordance with your Data Retention Policy. The information scope being deleted can be determined by the administrator in the following configuration: Delete User Policy Settings</p> <p>If a staff user's record is deleted, then the only information retained is the user's primary ID without any additional personal information.</p> <p>It is recommend that the primary ID be generic and not contain personal names that can easily be recognizable.</p>
<p>Right to Restrict Processing</p>	<p>Should a staff user wish to restrict the processing of their personal data, the individual's Alma user record could be deleted.</p> <p>In addition, customers have ability in Alma to provide shared/anonymous accounts to staff users who are entitled to restrict your processing of their data.</p> <p>Alma Analytics reports can be scheduled and sent to any email. (Schedule Alma Analytics feature). It has been a practice to use individual email addresses.</p> <p>Should a staff user wish to restrict the processing of their personal data, it is suggested that for Scheduling and Distributing Reports from Alma Analytics, 'group' or 'generic' email addresses be created to which the reports can be sent.</p> <p>User details that are extracted for Alma Analytics can be found in the Analytics - Users.</p> <p>Fields that contain identifying information of users can be anonymized when creating Alma Analytics reports. Anonymizing</p>

	<p>this data enables you to generate reports for statistics and trends without violating privacy concerns or local privacy-related laws. For more information concerning anonymization, see Anonymizing Alma Analytics Report Details and Configuring Anonymization. Additional information can be found in the Analytics - User details</p>
Right to Data Portability	<p>Alma offers the ability to export personal data in standard formats using standard API export functionality. Please see here information about the “Get User Details” API</p>
Right to Object	<p>Should a staff user wish to object to the processing of their personal data, the individual’s Alma user record could be deleted. In addition, customers have ability in Alma to provide shared/anonymous accounts to staff users who object to the processing of their personal data.</p>
Right related to Automated Decision Making and Profiling	<p>Any profiling or automated decision-making is determined and set by the customer. Generally, reports and task lists generated in Alma are designed to be used by humans for decision making.</p>

**Right related to
Data Breach
Notification**

Ex Libris has procedures for data breach handling including notification. In the case of a personal data breach, Ex Libris will, as soon as possible and within 72 hours after having become aware of it, notify the customer.

The notification will :

- Describe the nature of the personal data breach
- Communicate the name and contact details of the data protection officer
- Describe the likely consequences of the personal data breach
- Describe the measures taken or proposed to be taken by Ex Libris

When required by the GDPR, the institution/library as Data Controller, is responsible for notifying the Supervisory Authorities and the affected data subjects.

Ex Libris Security Incident Response Policy is available in the Ex Libris Knowledge Center - [here](#)

1. Data Fields of User in Alma

The following table lists the data fields in Alma that, based on the customer's decision, can be used to hold personal data provided by the customer. Next to each data field we have indicated whether the field is mandatory for normal Alma operations.

Category	Field	Mandatory	Functional Use in the System	Additional information
General Information	First name	Yes	<p>The name is shown in different interfaces to help the library staff identify the person to whom the service is given, for example, when the user approaches a circulation desk to services.</p> <p>The name may also be inserted into letters sent by the system to the patron.</p> <p>There is no other use of this field</p>	

Category	Field	Mandatory	Functional Use in the System	Additional information
	Middle name		<p>The name is shown in different interfaces to help the library staff identify the person to whom the service is given, for example, when the user approaches a circulation desk to get a service. The name may also be inserted into letters sent by the system to the patron</p> <p>There is no other use of this field</p>	
	Last name	Yes	<p>The name is shown in different interfaces to help the library staff identify the person to whom the service is given, for example, when the user approaches a circulation desk to get a service. The name may also be inserted into letters sent by the system to the patron</p> <p>There is no other use of this field.</p>	

Category	Field	Mandatory	Functional Use in the System	Additional information
	Primary identifier	Yes	Visible ID that is used to fetch a user record in the relevant functional context (e.g. when performing a loan). Functionally, it has the same use as any other user identifier – i.e. allows to uniquely identify a user as part of a given process, e.g. login, loan, integration with third party system.	
	Title		There is no functional use of this field. May be configured for use as a salutation in notifications that are addressed to the user.	
	PIN number		May be used by a selfcheck machine as a password in order to authenticate the self-check action (via SIP2 protocol). There is no other use of this field.	

Job category		May be used as input for determining fulfillment policies that will be applied to the user, and as an input that will determine automatic assignment of roles to a user.	Stores the job category definition to which the user belongs based on the Job Categories code table.
Job description		There is no functional use of this field.	A textual description of the user's job.
Gender		There is no functional use of this field.	Possible values: male, female, none, other
User group		The user group is used to assign fulfillment rules to the user, determining the fulfillment policies that will be applied to the user.	Stores the group with which the user is associated such as Faculty, Graduate, or Student.
Campus		The user's campus affiliation may be used to determine some attributes of fulfillment policies, such as allowed pickup locations for requests.	Stores the campus code of the user.
Preferred language		Determines the language that will be used by the system when sending notifications to the patron (if one of the supported languages is selected).	Stores the default language of the user.

	Birth date		Stores the birth date of the user. There is no other functional use for this field.	
	Expiration date		Determines when the user record will be considered inactive, i.e. the user will not be allowed to perform loans or be able to login (if Alma is used for authentication).	
	Purge date		Determines the date on which the record will be automatically deleted (unless the user has pending liabilities such as loans or fees).	
	Resource sharing library		The library that will manage resource sharing requests placed by the patron.	
	Cataloger level		Relevant for catalogers. A cataloger cannot override changes made by a cataloger with a higher level.	
	Selected Patron Letters		This field allows for opting out of specific library notices for specific patrons	A list of library notices will display.

Category	Field	Mandatory	Functional Use in the System	Additional information
Contact Information (multiple records)	Email types	Yes	This field defines whether the email is a work email or a home email. There is no functional use of this field.	
	Email address	Yes	The system will send library notices to this email address (if it is 'preferred', see next field).	The email address to which library notices will be sent.
	Preferred email	Yes	The system will send library notices only to the email address that is labeled as 'preferred'.	If this email should be used for library notices.
	Phone types		This field defines whether the phone is a work phone or a home phone. There is no functional use of this field.	
	Phone number		In case that library chooses to send phone notifications (i.e.: SMS) or contact the patron, this field will be used by the library. There is no functional use of this field.	The phone number by which the patron may be reached.

Preferred phone number		<p>This field defines whether the library should use this phone number for contacting the patron.</p> <p>There is no functional use of this field.</p>	
Preferred SMS		<p>If SMS is used, the system will use the phone number that is labeled as 'preferred' for creating the SMS.</p>	<p>If the library should use this phone number for sending SMS to the patron.</p>
Address types		<p>This field defines whether the address is a work address or a home address.</p> <p>There is no functional use of this field.</p>	
Address details (multiple fields)		<p>This field defines the physical address by which the patron may be reached.</p> <p>There is no functional use of this field.</p>	
Preferred address		<p>This field defines the preferred address to contact the patron. There is no functional use of this field.</p>	

Category	Field	Mandatory	Functional Use in the System	Additional information
Identifiers (multiple records)	Identifier Type		The intended use of the ID. IDs may be used by patrons for login, to fetch a user record, or by library systems for integration with the system (such as student IDs).	
	Value		The value is used during login for authentication, or in order to fetch a user record in the different functional contexts, for example for loaning an item to the patron.	IDs may be unique across the system, or be set to be unique only per their type.
	Note		An internal library field to add comments and notes. There is no functional use of this field.	
Notes (multiple records)	Note		Notes are displayed for the library staff when facing the patron (patron services workbench). The notes may also be displayed in the Primo interface (to the owner patron). There is no other functional use of this field.	

Blocks (multiple records)	Block description		The block description will be shown to the staff when the block blocks a patron's activity (such as loans). It will also be shown to the patron in Primo.	
	Expiry Date		The block will be ignored by the system after this date.	
	Note		An internal library field to add comments and notes. There is no functional use of this field.	
Fines and fees (multiple records)	Fine/Fee type		Notices may be sent based on a fee type, for example to all patrons who owe more than a defined amount of overdue fines, ignoring lost item fines.	The context of the fee – e.g. overdue loan fee, card renewal fee, lost item fee
	Comment		<p>This field is used for adding additional information about the fee, such as the reason for the fee. The field is displayed to users with the relevant privileges.</p> <p>There is no functional use of this field.</p>	

	Fee owner		Notices may be sent based on a fee owner, for example to all patrons who owe a given sum to a given library.	The library (or institution) that is owed the fee.
	Title		This field is used to determine whether the fee is linked to an item. This is the title of the item. There is no functional use of this field.	
	Item Barcode		This field is used to determine whether the fee is linked to an item, this is the barcode of the item. There is no functional use of this field.	
	Original Amount		The charged fee as the fee was created, before it was partly paid or waived.	

Category	Field	Mandatory	Functional Use in the System	Additional information
Statistics	Statistical Category		The field is used for Analytic reporting purposes only. There is no functional use of this field.	

	Category Type		The field is used for Analytic reporting purposes only. There is no functional use of this field.	
	Note		An internal library field to add comments and notes. There is no functional use of this field.	
Attachments	File name		The name given to an attached file. There is no functional use of this field.	
	Type		The type of the file attached (i.e.: WORD, PDF etc.). There is no other functional use of this field.	
	Size		The size of the attached file. There is no other functional use of this field.	
	URL		In the case where a URL link is used to a file. There is no other functional use of this field.	
	Notes		An internal library field to add comments and notes. There is no functional use of this field.	
Proxy	Proxy for		A user may borrow items on behalf of a user that is listed in this field.	

2. Staff Audit Trail

An audit trail is maintained for Staff users, for transactions such as loans, requests and PO lines. See [The Alma User Interface - History Tab](#). For examples, see [Managing Patron Services - Viewing Loan History](#). For cataloging in Metadata Editor see [Versioning](#).

For all other types of entities and transactions beyond the ones described below we retain only the creator and the last modifier. See [The Alma User Interface - Info icon](#).

Area	Transaction/Entity	Page
Acquisitions	Purchase Order Line	Details
	Invoice	Details
	License	Details
Resources Management	Collection Resource	Editor
	Bibliographic Record	Metadata Editor
	Authority Record	Metadata Editor
	Physical Holdings Record	Metadata Editor
	Physical Item	Editor
	Electronic Portfolio	Editor
	Electronic Service	Editor
	Electronic Collection	Editor
	Digital Representation Resource	Editor
Fulfillment	Loan Audit Trail	Patron Services
Resource Sharing	Borrowing Requests	Details
	Lending Requests	Details
Administration	User	Details
	Job	Monitor Jobs

Additional information can be found in Online Help:

- [Managing Users](#)
- [User Details in Analytics](#)
- [Data Privacy FAQs](#)