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

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," 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.

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

Table of Contents

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) takes effect in the European Union (EU). It replaces the Data Protection Directive (Directive"), which has 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 Voyager that can assist your organization in addressing data subject rights and requests as a *controller* and/or *processor* under the GDPR of personal data processed on Voyager.

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 Voyager, 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 Voyager, if you are running the software solution on premise, then the library/institution is the ***Data Processor*** as well as the *Data Controller*. If the software is running in the Ex Libris Cloud, then Ex Libris is the ***Data 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 either you or 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 Voyager

The following section describes the capabilities of Voyager 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 Voyager Functionality
Right to be Informed	Ex Libris provides comprehensive documentation regarding Voyager. 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 Voyager.
Right to Access	As Data Controller, you have full access to patron data in Voyager at all times and can search for, export, and delete portions of that data that relate to an individual patron at any time. In Voyager, the library staff manages the users and their information. In case of a patron's request to identify what categories of personal data are stored in Voyager, the patron can view select information via the OPAC. • **Personal information.** The Patron should log in to the OPAC and use the "My Account" feature in Voyager, located on the menu bar in WebVoyáge. My Library Card will show the patron what personal information is stored about them: a. Name b. Address c. Email d. SMS number e. Library account expiration date f. Library blocks g. Fines and fees h. Circulation charges, requests, and bookings • **Searches and saved records.** The patron should log in to Voyager and use the "My Searches", "My List" and "My

Account" features located on the menu bar in WebVoyáge. Search preferences, searches, and list items can be edited or removed by the patron.

Additional patron detail information can be provided by a library staff user. The patron record in Voyager contains personal and transactional information about the user. Details may include:

- **Contact Information –** Emails, phone numbers, and addresses
- **General Information –** such as department, major, and birth date
- **Identifiers –** In addition to the primary identifier, other identifiers can be associated with a user, such as a patron barcode, an institutional ID, and so forth.
- **Notes –** There can be multiple notes 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 current and historical fines and fees on the user
- **Statistics –** Counters and statistical categories assigned to the user specifically to be used in analytic reports
- **Proxy –** A proxy user can loan and return items on behalf of another user

The Voyager Circulation client and Voyager Reports can be used to report on additional user data elements to determine if they are used or not (e.g. if they are present in the data or null). For more details, reference the Voyager documentation here (Look in the *Circulation User's Guide* for your current version). See also Data Fields Used in Voyager below.

Patron information related to Acquisitions. If the patron has donated an item to the library, has requested the library purchase a title for the collection, or is a member of a serial routing list, information may have been saved in the Library's Acquisitions module.

- **Donor and Requestor information.** Donor and requestor information is saved in the Acquisitions module as a field on the line item. Voyager Access Reports can be used to run a "Donor List" report and a "Requestor List" report. The

	library staff member should review the report to see if the patron is listed. • **Routing Lists.** A patron may be a member of a serial routing list in Voyager. A staff member using the Voyager Acquisitions module can search Routing Lists by "Recipient – Patron", which will display a patron search window. If the patron is a member of a routing list, the search results will display in the Acquisitions module. For more details, reference the Voyager Acquisitions User's Guide on the Knowledge Center.
Right to Rectification	A patron may be able to update his own SMS number in Voyager via WebVoyáge or via an alternative discovery interface, depending on library policy. All other patron fields must be updated by an authorized staff member using the Voyager Circulation client. The patron should consult with a librarian to update his personal information. For more details, reference the Voyager documentation here (Look in the *Circulation User's Guide* for your current version). Donor, Requestor, or Routing List information may be updated by a member of the library staff using the Voyager Acquisitions client. The patron should consult with a librarian to update his personal information. For more details, reference the Voyager Acquisitions User's Guide on the Knowledge Center.
Right to Erasure (Right to be Forgotten)	A patron may be able to remove his own SMS number from Voyager via WebVoyáge or via an alternative discovery interface, depending on library policy. All other fields in the patron record can be deleted (where appropriate) by a librarian. Surname, name type, patron group, and line 1 of the permanent address are mandatory fields in Voyager. Removing the mandatory fields from Voyager requires the patron record to be deleted. Deleting the patron record will prevent the patron from requesting or borrowing materials from the library. The patron should consult with a librarian to have his personal information removed from Voyager. For more details, reference the Voyager documentation here (Look in the *Circulation User's Guide* for your current version).

Anonymization

Voyager circulation settings allow the library to control whether patron data is retained once materials have been returned to the library. If the data is retained, the library may choose to anonymize circulation transactions to protect the privacy of patrons' personal information.

The library can determine if patron data is being retained for historical transactions by checking a system setting in Voyager's System Administration module. The settings are saved under "System > Miscellaneous". Three options exist:

- Retain Patron ID for Circ History
- Retain Patron ID for Media Booking History
- Retain Patron ID for Distribution History

If these settings have a checkmark in front of them, patron data is being retained in the Circulation Transaction Archive and Distribution Archive tables when library materials are discharged or distributed. If these settings do not have a checkmark in front of them, the patron data is not saved when materials are discharged or distributed.

If the settings are enabled, the patron data can be anonymized by running a Circulation batch job.

If the patron ID is being retained in the Circulation history tables (for circulation or item distribution transactions), the library can run Retain Patron IDs (circjob 38) to remove the patron data from the archived transactions.

If the patron ID is being retained in the Media Booking history tables (for Media Booking transactions), the library can run Retain Patron IDs (mediajob 5) to remove the patron data from the archived transactions.

Deleting a Patron from Voyager

A patron record can be deleted via the Circulation client by a library staff member who has privileges to delete patron records. Before a patron record can be deleted, all items must be discharged, fines and fees resolved, and all outstanding requests will need to be cancelled. For details about deleting a patron through the Circulation client, reference the Voyager documentation here (Look in the *Circulation User's Guide* for your current version).

To delete a group of users at the same time, use the Patron Purge function (Circjob 39) that can be found in the Voyager batch jobs. The Patron Purge feature can be used with a text file of patron IDs to remove only the specified patron(s) from the system.

Additional batch jobs may be required to remove data before a patron record can be purged:

- Purge Universal Borrowing (UB) Stub Records (Circjob 29)
- Forgive Demerits (Circjob 37)
- Forgive Fines by Patron ID (Circjob 40)
- Forgive Fines by Create Date (Circjob 41)
- Forgive Fines by Patron Group and Expire Date (Circjob 42)

For more details about running batch jobs, refer to the Voyager documentation in the Knowledge Center (Look for the relevant batch jobs in the *Technical User's Guide* for your current version).

Users should be deleted in accordance with your Data Retention Policy.

Deleting a Donor or Requestor from Voyager

Donor or Requestor information can be deleted from the order line item by a library staff member using the Voyager Acquisitions module. The staff member should use the Donor List and Requestor List reports to identify line items to be updated, then update the necessary fields on the Delivery Options tab of the line item detail. Donors and Requestors should be deleted in accordance with your Data Retention Policy. For more details, refer to the Voyager Acquisitions User's Guide on the Knowledge Center.

Deleting a Routing List member from Voyager

Routing List members can be removed from Voyager by editing the Routing List in the Voyager Acquisitions module. Alternately, the patron will be automatically removed from any routing lists if the patron's record is deleted from Voyager using the Circulation module. Users should be deleted in accordance with your Data Retention Policy. For more details, refer to the Voyager Acquisitions User's Guide on the Knowledge Center.

Right to Restrict Processing	Should a Data Subject wish to object to the processing of their personal data, the individual's Voyager user record could be deleted. Libraries use patron's personal information to send them notices regarding library activity. These notices can include courtesy notices, item availability notices, recall notices, request cancellation notices, overdue notices, fines and fees notices, and statements of fines and fees. Voyager provides the ability for libraries to send notices via postal mail, email, or SMS. By default, notices are provided as printed forms. Patrons may request that certain types of notices be sent via email or, more recently, via SMS when a mobile number is provided. Conversely, patrons may request that mail not be sent to a temporary address, to an email address, or to an SMS number. To opt out of receiving notices at a temporary or email address, the "Hold Mail" box should be checked for the address(es) not to be used for notices. To opt out of SMS notices, the patron's mobile number should be removed from his patron record. Note: If mail is held for the patron's permanent address, the patron will be blocked from charging or renewing library materials. Additionally, Circulation staff operators can email patrons from the following areas within the Circulation module: • Patron record workspace • Charge workspace • Charged To dialog box of a charged item • Charged To dialog box of a charged reserve item To prevent a staff operator from emailing a patron from these workspaces, the patron's email address must be removed from his record. For details about editing an address or SMS number through the Circulation client, reference the Voyager documentation here (Look in the *Circulation User's Guide* for your current version).
Right to Data Portability	A single patron's record can be exported using the Patron Export web service and an XML document. Input can be provided with an XML document that contains the patron record ID and ID type (barcode, institution ID, or Voyager patron ID).

	The patron XSD, which describes the structure of the XML, is available in the Developer Network here. Once the patron record has been exported, a member of the library staff will be able to copy the record to portable media to provide to the patron. The patron will need to consult a member of the library staff to export the data. More information about patron export can be found in the *Voyager Technical User's Guide* on the Ex Libris Knowledge Center.
Right to Object	Voyager provides you with the full ability to determine which Patrons to include in the data load stored in Voyager. Patrons that exercise their "right to object" could be excluded from the patron data load into Voyager. Patrons may also be deleted as described above.
Right related to Automated Decision Making and Profiling	Any profiling or automated decision-making is determined and set by the customer. Generally, reports and task lists generated in Voyager are designed to be used by humans for decision making.
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

2. Rights of Data Subjects – Staff

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

Data Subject Right	Corresponding Voyager Functionality
Right to be Informed	Ex Libris provides comprehensive documentation regarding Voyager. 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 Voyager.
Right to Access	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). The staff data stored is dependent on the roles and activities of the staff user: • Personal information ○ User Name (first, middle initial, last) ○ User ID ○ User Password • Audit on staff user activity in the system ○ Bib records created by operator ○ Patrons created by operator Staff users' personal information can be accessed only by an authorized Voyager system administrator using the Voyager System Administration module. More information about staff operators can be found in the *Voyager System Administration User's Guide* on the Ex Libris Knowledge Center. Audit reports of user information can be accessed using the Voyager Reports module to generate the reports referenced above. Additional audit trail information may be identified by the library by creating ad hoc reports within the Voyager Access Reports module. More information about Voyager's Prepackaged Access Reports can be found in the *Voyager Reporter User's Guide* on the Ex Libris Knowledge Center.

Right to Rectification	A user can ask that his/her personal information be corrected or updated as necessary. More information about staff operators can be found in the *Voyager System Administration User's Guide* on the Ex Libris Knowledge Center.
Right to Erasure (Right to be Forgotten)	Should a staff user wish to erase their personal information, the individual's Voyager user record can be deleted from the system. Note that, for integrity purposes, existing audit trail information cannot be removed from the system. More information about staff operators can be found in the *Voyager System Administration User's Guide* on the Ex Libris Knowledge Center.
Right to Restrict Processing	Should a staff user wish to restrict the processing of their personal data, the individual's Voyager user record could be deleted. More information about staff operators can be found in the *Voyager System Administration User's Guide* on the Ex Libris Knowledge Center.
Right to Data Portability	A staff user's personal information (first name, middle initial, last name, and ID) can be copied from the System Administration module and pasted into a text file. For security purposes, the user's password is stored encrypted in the Voyager database and cannot be viewed or exported. More information about staff operators can be found in the *Voyager System Administration User's Guide* on the Ex Libris Knowledge Center.
Right to Object	Should a staff user wish to object to the processing of their personal data, the individual's Voyager user record could be deleted. In addition, customers have ability in Voyager to provide shared/anonymous accounts to staff users who object to the processing of their personal data. More information about staff operators can be found in the *Voyager System Administration User's Guide* on the Ex Libris Knowledge Center.
Right related to Automated Decision Making and Profiling	Any profiling or automated decision-making is determined and set by the customer. Generally, reports and task lists generated in Voyager are designed to be used by humans for decision making.

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

Data Fields Used in Voyager

Patron	Data
	Name (title, first, middle, surname)
	SMS Number
	Department
	Major
	Birthdate
	SSN
	Institution ID
	Barcode
	Patron Group

	Multiple Addresses (permanent + up to 8 temporary and/or email addresses)
	Multiple Phone Numbers (primary, mobile, fax, other)
	Registration Date
	Expiration Date
	Purge Date
	Multiple Notes
	Charged Items
	Requested Items
	Fines and Fees (current and historical)
	Patron Current Activity (charges, call slips, short loans, holds, recalls, bookings)
	Patron Historical Activity (charges, claims returned, lost items, self-shelves, call slips placed, short loans placed, unclaimed short loans, item distributions, historical bookings, cancelled bookings, unclaimed bookings, booking counters)
	Statistical Categories
	Suspension Date
	Demerits
	PIN
	Saved Searches
	Saved Bibliographic Records

Staff Users	Data
	User Name
	User password
	Display Name (UserID)