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

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 Summon that can assist your organization in addressing data subject rights and requests as a *controller* under the GDPR of personal data processed on Summon.

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 Summon, 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 Summon, 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 Summon

The following section describes the capabilities of Summon 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 Summon Functionality
Right to be Informed	Ex Libris provides comprehensive documentation regarding Summon. 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 Summon.
Right to Access	Information about the Patron is not stored in Summon. NOTE: Summon integrates with a variety of platforms, including Alma and RefWorks that includes personal information, however, this information is not collected by Summon and cannot be corrected or deleted using Summon.
Right to Rectification	Patron data in Summon must be rectified in the originating system, such as Alma and RefWorks.
Right to Erasure (Right to be Forgotten)	Patron data in Summon must be erased in the originating system, such as Alma and RefWorks.
Right to Restrict Processing	Patron data in Summon must be removed from processing or deleted in the originating system, such as Alma and RefWorks.
Right to Data Portability	Because no personal data resides in Summon, there is currently no need for mechanisms for data portability.
Right to Object	Patron data in Summon must be removed from processing or deleted in the originating system, such as Alma and RefWorks.
Right related to Automated Decision Making and Profiling	Any profiling or automated decision-making is determined and set by the customer and is done using data that is not associated with any individual. Generally, reports generated in Summon are designed to be used by humans for decision making purposes.

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 Summon that can assist customers in complying with the rights of the data subjects with respect to its staff.

Data Subject Right	Corresponding Summon Functionality
Right to be Informed	Ex Libris provides comprehensive documentation regarding Summon. 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 Summon.
Right to Access	Staff user information can be viewed by Staff depending on their individual level of access authority. To view, correct, or delete Staff information, the Staff member should contact the system administrator.

Right to Rectification	A staff user with the relevant privileges can edit and correct inaccurate personal data using existing standard functionality.
Right to Erasure (Right to be Forgotten)	To view, correct, or delete Staff information, the Staff member should contact the system administrator.
Right to Restrict Processing	Should a Data Subject object to the processing of their personal data, the individual's user record could be deleted.
Right to Data Portability	There is no data stored in Summon that would require data portability; Summon only stores an individual's email address, name and password for use in the administrative console and for emailing reports.
Right to Object	Staff members that exercise their "right to object" could be deleted from Summon.
Right related to Automated Decision Making and Profiling	Any profiling or automated decision-making is determined and set by the customer and is done using data that is not associated with any individual. Generally, reports generated in Summon are designed to be used by humans for decision making purposes.
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