Ex Libris and the General Data Protection Regulation (GDPR)

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 applicability 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 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

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 the 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 the GDPR might apply to you and your organization. We encourage you to work with a legally qualified professional to discuss the GDPR, how it applies specifically to your organization, and how best to ensure compliance.

Introduction

A new privacy law called the General Data Protection Regulation (GDPR) is applicable as of May 25th, 2018 in all member states of the European Union (EU), strengthening and harmonizing individuals' data-protection rights throughout the European Union. The regulation puts a strong emphasis on transparency – understanding what data is being used, how it is being used, and how it is protected. As more particularly set out in Article 3 of the GDPR, the GDPR generally applies to companies and organizations that collect or process data from EU residents.

Ex Libris is committed to supporting GDPR compliance across our products and services. We have closely analyzed the requirements of the GDPR, and our engineering, product, security and legal teams have worked to align our procedures, services, documentation, and contracts to support compliance with the GDPR. We continue to support customers in their GDPR compliance journey, using our strong foundation of certified security and data protection. Ex Libris understands that compliance is a shared responsibility with our customers, and we are committed to working with you to comply with the GDPR and future privacy requirements.

This paper is aimed at informing Ex Libris customers about the various GDPR compliance activities of Ex Libris (company, products and services). For detailed product functionality related to GDPR compliance, please consult the product-specific GDPR documentation available on the Ex Libris Trust Center, at https://trust.exlibrisgroup.com/gdpr/.

Is Ex Libris a Data Processor or a Data Controller?

The manner in which the GDPR will impact you as an Ex Libris customer will depend in part on the way in which our products and services are deployed and used in your organization. This is because the GDPR makes a distinction between two types of roles:

- "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.
- "Processor" means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

Is Ex Libris a Processor or Controller?

Ex Libris operates as both a Processor and a Controller when considering GDPR compliance. For example:

- Ex Libris is a Processor in cases where Ex Libris handles personal data on behalf of its customers (e.g. for our SaaS services – including our multi-tenant and hosted products).
- Ex Libris is a Controller in cases where Ex Libris handles any personal data on its own behalf (e.g. processing our employee data for our own accounts and purposes, promoting our products and services through marketing etc.).

How is Ex Libris implementing GDPR compliance?

Ex Libris welcomes the GDPR as an important step forward in streamlining data protection requirements across the EU and as an opportunity for Ex Libris to deepen its commitment to data protection.

Many of the main concepts and principles of the GDPR are similar to existing EU data privacy laws. Therefore, much of our current approach will remain valid under the GDPR. However, the GDPR introduces new elements and important enhancements that require detailed consideration by all organizations involved in processing personal data.

Ex Libris has been working towards compliance with the GDPR since its adoption in the spring of 2016. We established a global project to prepare for the GDPR, both for our internal processes and for our commercial offerings. Ex Libris appreciates that our customers have requirements under the GDPR that are directly impacted by their use of Ex Libris products and services, and Ex Libris is committed to helping our customers meet their requirements under the GDPR.

Our approach to data privacy is comprehensive and holistic, leveraging the GDPR to influence our approach across the globe – this is not just an EU initiative for Ex Libris. We have touched many parts of the organization to get ready for the GDPR.

Here are some highlights of the tasks we have performed to get ready for the GDPR:

1. Planning, Training & Awareness

1.1. Reviewed the GDPR and its requirements, and ensured the key decision makers and privacy/security-related personnel are made aware of the GDPR's requirements and overall impact on Ex Libris processing activities.

1.2. Established a global readiness program tasked with identifying the key impacts of the GDPR across Ex Libris business and preparing Ex Libris internal processes and commercial offerings for compliance with the GDPR.

1.3. Established a cross-functional team to manage the GDPR readiness program. In addition, a senior-level steering team was established to oversee the program and ensure it remained on track.

1.4. Launched an enhanced employee training and awareness program, supplementing existing employees training modules with GDPR-specific content. In addition to these training requirements, Ex Libris conducts ongoing awareness initiatives on a variety of topics, including data protection, security and privacy.

2. Gap Assessment

2.1. Conducted an inventory and mapping of personal data processed by Ex Libris products and services.

2.2. Identified, mapped, and documented the systems that process personal data, subject to the GDPR, to ensure adequate controls are in place to protect this data.

2.3. Assessed gaps between current Ex Libris policies, procedures, and practices and compliance requirements under the GDPR.

2.4. Conducted a data mapping exercise and Privacy Impact Analysis (PIAs) of relevant products and services in light of GDPR requirements.

3. Contracting and Policies

3.1. Reviewed and revised our customer and vendor facing contractual documentation to reflect our and our customers' respective obligations under the GDPR.

3.2. Reviewed our contracts with sub-processors to align them with the requirements imposed by the GDPR, and to confirm that our sub-processors understand their responsibilities and are fully committed to meeting them.

3.3. Identified cross-border data flow and reviewed mechanisms in place.

3.4. Reviewed our public-facing privacy policies, marketing materials, and other notices and updated them to satisfy the GDPR's transparency requirements.

3.5. Reviewed and updated policies and procedures covering data subjects' rights.

4. Governance and Processes

4.1. Developed a range of internal communication and training initiatives to ensure employees are made aware of the GDPR duties, obligations, and proper data use.

4.2. Updated HR policies to align with the GDPR.

4.3. Improved our procedures where necessary, to allow us to respond appropriately to data subject requests.

4.4. Designated a Data Protection Officer (DPO) to oversee GDPR compliance.

5. Security

5.1. Reviewed our ISO 27001-compliant data security standards and processes and our privacy policy to ensure they meet the requirements imposed by the GDPR.

5.2. Embedded the principle of "Privacy by Design" into our products and development lifecycle.

5.3. Records of processing activities – created a register of data processing activities.

5.4. Reviewed the security protocols of our internal information systems (CRM, website, marketing tools, etc.) for compliance with the GDPR.

5.5. Carried out a review of data retention policies across internal information systems.

5.6. Updated our policies and procedures to comply with the personal data breach notification requirements under the GDPR.

6. Working with customers

6.1. Worked with our customers to answer their questions and provide resources and helpful information about privacy and the GDPR, including white papers.

6.2. Released an updated Data Processing Addendum with provisions to assist our customers with their GDPR compliance.

6.3. Provided the necessary information to assist our customers to create (where applicable) Data Protection Impact Assessments (DPIAs).

6.4. Reviewed and revisited our processes for receiving and responding to customers' requests to assist with data subject requests.

Regulation Articles and Ex Libris Compliance

We have analyzed the requirements contained in each GDPR article and provide Ex Libris' insights and statements on all articles in the table below. As noted above, for product information, please refer to the GDPR product-specific documentation ("What You Need to Know About Addressing GDPR Data Subject Rights").

Topic	GDPR Article	Ex Libris Statement
Subject matter and objectives	1	**Outline/Summary:** Article 1 provides the purpose of the GDPR. **Ex Libris Statement:** Ex Libris and its affiliates are committed to compliance with all relevant EU and Member State laws in respect to personal data and to the protection of the "rights and freedoms" of individuals whose information Ex Libris processes in accordance with the General Data Protection Regulation (GDPR).
Material scope	2	**Outline/Summary:** Article 2 addresses the activities that are within or outside the scope of the GDPR. **Ex Libris Statement:** We encourage you to work with a legally qualified professional to discuss the GDPR, how it applies specifically to your organization, and how best to ensure compliance.
Territorial scope	3	**Outline/Summary:** Article 3 addresses the application of the GDPR to entities within and outside the European Union. **Ex Libris Statement:** Ex Libris and its group companies (affiliates) have been preparing for the implementation of the GDPR. We support the GDPR accountability principle and understand we have an obligation to comply with the regulation's requirement within its territorial scope.

Definitions	4	**Outline/Summary:** The key terms such as "personal data," "processing," "controller," "processor," and "consent," which are used throughout the text of the GDPR, are defined in this article. **Ex Libris Statement:** As you read through this paper, keep in mind that in cases where Ex Libris handles personal data on behalf of its customers, including our multi-tenant and hosted products, our customers' compliance with the GDPR generally involves its role as a "controller" and the Ex Libris role as a "processor". We act as a data processor in respect to any personal data which our customers upload onto our cloud-based SaaS services (such as Alma). In providing our service, we do not own or make decisions about the use of the personal data stored or processed on our SaaS services. We do not use this data for our own purposes. In fact, to the extent we do access this data, it is only as reasonably necessary in order to provide our customer with our services (which may include responding to support requests) or as required by law. It is up to our customers to make sure that they comply with the relevant GDPR requirements before storing and processing personal data on our SaaS services.
Principles relating to processing of personal data	5	**Outline/Summary:** Article 5 sets out the general principles that all processing activities must abide by, including: "lawfulness, fairness and transparency"; "purpose limitation"; "data minimization"; "accuracy"; "storage limitation"; "integrity and confidentiality" and "accountability." **Ex Libris Statement:** Ex Libris engages in ongoing comprehensive cross-company activities to comply with data protection principles. Ex Libris is implementing updated data protection policies, reinforcing adherence to codes of conduct, implementing technical and organizational measures, and adopting techniques such as data protection by design. Ex Libris also publishes and updates a wide range of security and privacy documentation evidencing these activities, including data processing impact assessments for many of its products and services, breach notification procedures, guidance for meeting data subject rights requests, and incident response plans.
Lawfulness of processing	6	**Outline/Summary:** Article 6 provides legal grounds on which personal data can be processed.

		Ex Libris Statement: The customer (controller) shall be responsible for having all necessary rights to collect and process and to allow collection and processing of all personal data stored in the Ex Libris SaaS services. Ex Libris (the processor) processes such data pursuant to its contracts with the customer.
Conditions for consent	7	**Outline/Summary:** Article 7 sets out the conditions for consent when a controller is relying on consent as a legal basis for processing personal data. **Ex Libris Statement:** Obtaining the consent of the data subject when required is the responsibility of the customer as the controller. The controller shall be responsible for having all necessary rights to collect and process and to allow collection and processing of all personal data stored in the Ex Libris SaaS service.
Conditions applicable to child's consent in relation to information society services	8	**Outline/Summary:** Article 8 provides special legal condition for children's consent **Ex Libris Statement:** Obtaining the consent of the data subject when required is the responsibility of the customer as the controller. The controller shall be responsible for having all necessary rights to collect and process and to allow collection and processing of all personal data stored through the Ex Libris SaaS service.
Processing of special categories of personal data	9	**Outline/Summary:** Article 9 establishes a special legal regime for categories of data that are considered especially sensitive. **Ex Libris Statement:** Ex Libris contracts generally do not allow customers using our SaaS products and service (such as Alma) to store or process special categories of personal data ("sensitive data") in our cloud services. Specifically, the storing or processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation is prohibited.
Processing of personal data relating to criminal convictions and offences	10	**Outline/Summary:** Article 10 provides the legal basis upon which personal data relating to criminal convictions and offences may be processed.

		Ex Libris Statement: Ex Libris does not permit the storage or processing of personal data relating to criminal convictions and offences on its SaaS services.
Processing which does not require identification	11	**Outline/Summary:** Article 11 stipulates when a controller has no obligation under the GDPR to keep personal data and when the identification of the data subject is no longer necessary. **Ex Libris Statement:** Ex Libris acts as a data processor in providing its products and SaaS services. The customer (the controller), and not Ex Libris, determines whether to retain the information necessary for identifying its data subjects.
Transparent information, communication and modalities for the exercise of the rights of the data subject	12	**Outline/Summary:** Article 12 contains detailed requirements regarding the controller's obligation to provide transparent information and communication to the data subject and regarding the modalities for the exercise of the rights of the data subject. **Ex Libris Statement:** Provision of necessary information to data subjects is the responsibility of the customer as controller. Upon request, Ex Libris will provide our customers with reasonable assistance to the extent necessary for the controller to respond to data subject requests to exercise one or more of their rights under the GDPR.
Information to be provided where personal data is collected from the data subject	13	**Outline/Summary:** Article 13 provides that where personal data relating to data subjects is collected, controllers must provide certain minimum information to those data subjects through an information notice. It also sets out requirements for timing of the notice and identifies when exemptions may apply. **Ex Libris Statement:** Provision of necessary information to data subjects is the responsibility of the customer as the controller. Upon request, Ex Libris will provide customers of the SaaS Services with assistance to the extent necessary for the controller to respond to data subject requests to exercise one or more of their rights under the GDPR.
Information to be provided where personal data has not been obtained from the data subject	14	**Outline/Summary:** Article 14 specifies what information is required to be provided to data subjects when that information is not obtained by the controller. **Ex Libris Statement:** Provision of necessary information to data subjects is the responsibility of the customer as the controller. Upon request, Ex Libris will provide customers of the SaaS Services with

		assistance to the extent necessary for the controller to respond to data subject requests to exercise one or more of their rights under the GDPR.
Right of access by the data subject	15	**Outline/Summary:** Article 15 addresses the right of data subjects to obtain confirmation of whether their personal data is being processed and where it is being processed and to have access to the data. Additionally, it lists further information that should be supplied. **Ex Libris Statement:** The controller (customer) remains in control of its data. Ex Libris SaaS services enable customers to provide a copy of personal data to the data subject (patron or library personnel). Upon request, Ex Libris will provide customers of the SaaS Services with assistance to the extent necessary for the controller to respond to data subject requests to exercise one or more of their rights under the GDPR.
Right to rectification	16	**Outline/Summary:** Article 16 stipulates the data subject's right to obtain the rectification of inaccurate or incomplete personal data. **Ex Libris Statement:** The customer remains in control of its data. Ex Libris provides customers with tools and instructions for updating data subject information stored in the SaaS Services to assist the customer in meeting this responsibility to the user (data subject) when requested. The customer remains responsible for communicating with the data subject and for correcting their personal information.
Right to erasure ("right to be forgotten")	17	**Outline/Summary:** Article 17 addresses the right of data subjects to request the erasure of personal data from the data controller based on certain grounds. **Ex Libris Statement:** The customer remains in control of its data. Ex Libris products and SaaS services enable customers to implement methods for erasure of the data subject's personal information, as appropriate. For details on each product, please review the product-specific Ex Libris document. These documents include instructions on how to delete information pertaining to the data subject to assist the Ex Libris customer in meeting this obligation.
Right to restriction of processing	18	**Outline/Summary:** Article 18 addresses the right of a data subject to obtain a restriction on the processing of personal data in cases such as pending verification of a legal ground to process or where accuracy of the data is disputed.

		Ex Libris Statement: The customer remains in control of its data. Ex Libris products and SaaS services allow the customer to implement methods to restrict processing of the data subject's personal information, as appropriate.
Notification obligation regarding rectification or erasure of personal data or restriction of processing	19	**Outline/Summary:** Article 19 creates an obligation to notify each recipient to whom data has been disclosed of any rectification, erasure or restriction of processing and to inform data subjects about such recipients upon request. **Ex Libris Statement:** The customer as the controller remains responsible for communicating with the data subject. Upon customer request, Ex Libris will provide reasonable assistance in responding to data subject requests.
Right to data portability	20	**Outline/Summary:** Article 20 provides data subjects with a right to, in certain circumstances, receive personal data concerning him or her, in a structured and commonly used and machine-readable format, and to transmit such data to another data controller. **Ex Libris Statement:** The controller (customer) remains in control of its data. Ex Libris provides tools and techniques within the SaaS services allowing the customer to export personal data in a structured, commonly used and machine-readable format.
Right to object	21	**Outline/Summary:** Article 21 addresses the right of data subjects to object to the processing of their personal data. **Ex Libris' Statement:** The customer remains in control of its data. Ex Libris products and SaaS services allow the customer to implement methods to remove personal data of the data subject or restrict processing of the data subject's personal information, as appropriate.
Automated individual decision-making, including profiling	22	**Outline/Summary:** Article 22 addresses the right of data subjects to not be subject to a decision based solely on automated processing, where such decisions would have a legal or significant effect concerning the data subject. **Ex Libris Statement:** Any profiling or automated decision-making is determined and set by the customer. Generally, reports and task lists generated in Ex Libris products and SaaS services are designed to be used by humans for decision-making.

Restrictions on the scope of data subject right	23	**Outline/Summary:** Article 23 provides that Union or Member State law may create restrictions on the scope of data subject rights, and thus the obligations of data controllers. **Ex Libris Statement:** Ex Libris and its affiliates are committed to complying with all applicable laws and regulations (including without limitation, privacy laws and regulations) in connection with the operation of the SaaS Services.
Responsibility of the controller	24	**Outline/Summary:** Article 24 requires the data controller to implement appropriate technical and organizational measures to ensure and be able to demonstrate compliance with the GDPR. **Ex Libris Statement:** In addition to Ex Libris compliance obligations under the GDPR as a processor of customers' personal data, Ex Libris supports our customers in meeting their obligations under the GDPR in this regard. Ex Libris is ISO 27001, ISO 27017, ISO 27018 and ISO 22301 certified, and uses SSAE-18 certified data center facilities.
Data protection by design and by default	25	**Outline/Summary:** Article 25 imposes a general duty for the controller to implement measures encouraging privacy by design and privacy by default **Ex Libris Statement:** Ex Libris products and services are developed utilizing the Ex Libris Secure Development Lifecycle, which incorporates privacy-by-design and privacy-by-default methodologies, and are in accordance with Ex Libris privacy policies. Furthermore, Ex Libris is audited at least annually against several global data privacy and security standards, including ISO 27018 (privacy) and ISO 27001 (security).
Joint controllers	26	**Outline/Summary:** Article 26 provides that where two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers. **Ex Libris Statement:** Upon request, Ex Libris can assist in assessing its responsibilities in a joint controller situation.
Representatives of controllers or processors not established in the Union	27	**Outline/Summary:** Article 27 obliges controllers and processors who are not established in the EU, but offer goods and services or profile EU citizens, to appoint a representative in the EU.

		Ex Libris Statement: Ex Libris Ltd. (Israel) has designated Ex Libris (Deutschland) GmbH as its representative in the European Union.
Processor Obligations	28	**Outline/Summary:** Article 28 determines the obligations of parties which are acting as personal data processors. **Ex Libris Statement:** Please see Ex Libris statements for section 28.1, 28.2, 28.3 and 28.4 below
Use only processors guaranteeing appropriate measures	28.1	**Outline/Summary:** The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures. **Ex Libris Statement:** Ex Libris has published DPAs which include a description of appropriate measures. Ex Libris also maintains ISO 27001:2013 certification. Central to this certification is our Information Security Management System (ISMS) which protects the confidentiality, integrity, and availability of information within our SaaS services. Our ISMS is regularly tested and externally audited each year as a requirement of maintaining our certification.
Prior authorization to use sub-processors	28.2	**Outline/Summary:** The processor shall not engage another processor without prior written authorization. **Ex Libris Statement:** Ex Libris group companies (affiliates under common ownership) directly conduct the data processing activities required to provide Ex Libris products and SaaS services. We do engage a number of trusted third-party vendors to provide specific services, such as data center facilities. We comply with GDPR requirements in this regard by making information available about Ex Libris group sub-processors and third party vendors and including required commitments and consents in our data processing agreements. The procedure to replace or appoint a new sub-processor is covered within our Data Processing Agreement with our customers. We provide our customers (controllers) advance notification of any changes or additions and the opportunity to object on a reasonable basis.
Processing governed by Contract	28.3	**Outline/Summary:** Processing shall be governed by a contract (Data Processing Agreement - DPA). **Ex Libris Statement:** As the data processor and in recognition of this mutual obligation, Ex Libris has prepared, published, and made

		available GDPR-compliant Data Processing Agreements for each of its products and service groups for execution by customers, in the form of Addenda to existing and future customer license and services agreements. These DPAs have been prepared under the supervision of recognized European data privacy counsel and experts to meet the requirements of Article 28.3 and the GDPR in general. As required by the GDPR, the DPAs are geared specifically to the purposes, processes, and intended data subjects of the services provided by Ex Libris.
Processing only on the written instructions of the controller	28.3 (a)	**Outline/Summary:** Under Article 28.3(a) the DPA shall stipulate that the processor will perform processing only on documented instructions, including regarding international transfer (unless, subject to certain restrictions, it is legally required to transfer to a third country or international organization). **Ex Libris Statement:** Any personal data that a customer (controller) and its users put into Ex Libris products and SaaS services will only be processed in accordance with the customer's instructions, as described in our services agreement and data processing agreements.
Personnel confidentiality commitments	28.3 (b)	**Outline/Summary:** Under Article 28.3(b) the DPA shall stipulate that the processor should ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. **Ex Libris Statement:** All Ex Libris personnel who are authorized to process personal data have committed themselves (through employment and confidentiality agreements and acknowledgements) to the confidentiality and security of personal data. We include commitment relating to confidentiality in our data processing agreements.
Appropriate security measures	28.3 (c)	**Outline/Summary:** Under Article 28.3(c) the DPA shall stipulate that the processor should take all measures required under the security provisions (Article 32). **Ex Libris Statement:** Ex Libris has published a description of appropriate technical and security measures in its DPAs and maintains ISO 27001:2013 certification.
Using sub-processors	28.3 (d)	**Outline/Summary:** Under Article 28.3(d) the DPA should stipulate that the processor will only use a sub-processor with the controller's consent (specific or general, although where general consent is obtained, processors must notify controllers of such

		changes, giving them an opportunity to object) and that the same contractual obligations apply to sub-processors. **Ex Libris Statement:** The DPA includes the required commitment to consent regarding sub-processors and a commitment to inform the customer of any intended adjustment of processing roles and/or addition of sub-processors, thereby giving the customer (controller) opportunity to reasonably object to such adjustment and/or addition.
Processor assistance with Data Subjects' Requests	28.3 (e)	**Outline/Summary:** Under Article 28.3(e) the DPA should stipulate that the processor assist the controller in meeting the controller's obligations to data subjects under chapter III of the GDPR. **Ex Libris Statement:** Ex Libris provides our customers (controllers) with instructions regarding the use of tools within the Ex Libris SaaS Services to allow them to access, rectify, erase, and block personal data relating to data subjects that is stored on the SaaS services, and to export such personal data in a structured, commonly used and machine-readable format. If Ex Libris receives a request from our customer's data subject to exercise one or more of his/her rights under the GDPR, Ex Libris will redirect the data subject to make his/her request directly to our customer. In addition, to the extent that our customer, in its use of the SaaS Services, does not have the ability to address a data subject request, Ex Libris shall upon request, provide reasonable assistance in responding to such data subject request to the extent Ex Libris is legally permitted to do so and the response to such data subject request is required under the GDPR.
Assisting the controller with Articles 32-26	28.3 (f)	**Outline/Summary:** Under Article 28.3(f) the DPA should stipulate that the processor shall assist the controller in complying with the obligations relating to security, breach notification, DPIAs and consulting with supervisory authorities (Articles 32-36). **Ex Libris Statement:** Ex Libris will assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR – security, notification of data breaches, communication of data breaches to individuals, data protection impact assessments and, when necessary, consultation with the supervisory authorities, taking into account the nature of processing and the information available to Ex Libris.
Deletion and Return of personal data	28.3 (g)	**Outline/Summary:** Under Article 28.3(g) the DPA should stipulate that the processor will delete or return (at the controller's choice) all

		personal data at the end of the agreement (unless storage is required by EU/member state law). **Ex Libris Statement:** At contract termination or expiration, Ex Libris will, at the choice of the controller, make all the controller's personal data available to the controller and, unless otherwise agreed or required by applicable law, will delete personal data within a reasonable and appropriate period after it has made the data available to the controller.
Controller's right to audit	28.3 (h)	**Outline/Summary:** Under Article 28.3(h) the DPA shall stipulate that the processor will make all information necessary to demonstrate compliance available to the controller and allow/contribute to audits (including inspections). **Ex Libris Statement:** Ex Libris conducts regular internal audits to ensure physical, logical, and information security standards are being followed as per the ISO 27001 standard. Ex Libris also undergoes external audits on an annual basis, as part of its continued compliance to ISO 27001 certification requirements. In addition, a third-party vendor conducts an annual Vulnerability Assessment Penetration Testing (VAPT) of Ex Libris SaaS services to identify and patch any weaknesses or vulnerabilities. As per the GDPR and Ex Libris DPAs, Ex Libris shall make available to our customers (controllers) information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted on behalf of the controller.
Processor engaging with sub-processor	28.4	**Outline/Summary:** Under Article 28.4, in a case where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the DPA shall be imposed on that other processor. **Ex Libris Statement:** Ex Libris engages with sub-processors on the basis of written contracts that impose data protection obligations on the sub-processor no less protective of personal data than those imposed on Ex Libris in the DPAs.
Processing under the authority of the controller or processor	29	**Outline/Summary:** Article 29 provides a general duty for the processor to only process data under the instruction of the controller.

		Ex Libris Statement: This requirement is covered in the contracts signed between Ex Libris and the customer. Ex Libris only processes personal data for the purposes detailed in the contract and the relevant DPA.
Records of processing activities	30	**Outline/Summary:** Article 30 sets out a detailed list of information that must be maintained as records of processing activities carried out by and on behalf of the controller, as well as the requirement to make these records available to data subjects and Supervisory Authorities upon request. **Ex Libris Statement:** Ex Libris will register all processing activities and document them in accordance with the GDPR requirements.
Cooperation with the supervisory authority	31	**Outline/Summary:** Article 31 introduces an obligation on controllers, processors, and representatives to cooperate with supervisory authorities in the performance of their tasks. **Ex Libris Statement:** When requested, Ex Libris will cooperate with the personal data supervisory authorities.
Security of processing	32	**Outline/Summary:** Article 32 requires an "appropriate" level of security, taking into account the state of the art, costs of implementation, scope and purpose of the processing activities, and risk of varying likelihood and severity to individuals' rights and freedoms. **Ex Libris Statement:** Ex Libris has published a description of appropriate technical and security measures in its DPAs. Ex Libris also maintains ISO 27001:2013 certification. This certification requires annual external audits to validate that all required security measures and mitigations are in place. The security measures employed by Ex Libris include access rights control, data encryption means, redundant storage media and servers meant to ensure availability and continuity of service, a backup strategy meant to enable rapid recovery in case of any physical or technical incident, continuous monitoring of production servers, penetration testing, and vulnerability scans.
Notification of a personal data breach to the supervisory authority	33	**Outline/Summary:** Article 33 makes it mandatory to notify supervisory authorities in the event of a data breach that poses a "risk of harm." In addition, this Article sets out detailed content requirements for the notification letter.

		Ex Libris Statement: Under the GDPR, we must notify any personal data breach to the controller without undue delay. Ex Libris therefore has processes and procedures in place for identifying, reviewing, and promptly reporting data breaches to the relevant controller. 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 We note again that Ex Libris employs comprehensive technical and organizational security measures to mitigate against a data breach.
Communication of a personal data breach to the data subject	34	**Outline/Summary:** Article 34 requires controllers to notify data subjects of breaches that result in a "high risk" for the rights and freedoms of individuals. **Ex Libris Statement:** Ex Libris will assist the controller (customer) in meeting its obligation, taking into account the nature of the processing and information available to Ex Libris.
Data Protection Impact Assessment (DPIA)	35	**Outline/Summary:** Article 35 requires controllers to assess the impact of processing operations on the protection of personal data in cases where the processing is likely to result in a high risk for the rights and freedoms of data subjects. **Ex Libris Statement:** Ex Libris will assist the controller, where necessary and upon request, in meeting its obligation in carrying out Data Protection Impact Assessments, taking into account the nature of the processing and information available to Ex Libris. We note that, as part of Ex Libris GDPR-readiness activities, Ex Libris commissioned, on a voluntary basis, data protection impact assessments on various internal systems and customer products, which were carried out by an external independent organization (KPMG).
Prior Consultation with Supervisory Authority	36	**Outline/Summary:** Article 36 requires data controllers to consult with the supervisory authority when a DPIA indicates that processing would result in a high risk to data subjects.

		Ex Libris Statement: Ex Libris shall assist the controller, where necessary and upon request, in meeting its obligation to carry out such consultations, taking into account the nature of the processing and information available to Ex Libris.
Designation of the data protection officer	37	**Outline/summary:** Article 37 provides that the data controller and the data processor shall designate a data protection officer ("DPO") in specified circumstances. **Ex Libris Statement:** Ex Libris and its affiliates have appointed a data protection officer (DPO) to act as a primary contact for data privacy-related matters and to advise the company on compliance with the GDPR. The Ex Libris DPO is responsible for overseeing the data protection strategy as well as its implementation in order to ensure compliance with data protection requirements. The DPO is also a contact person for supervisory authorities (SAs) for communication and notification of personal data breaches, audit reports, results of privacy impact assessments, etc. The Ex Libris DPO may be reached at dpo@exlibrisgroup.com or another such address as occasionally published by Ex Libris. Further information regarding the DPO can be found on the Ex Libris public website at https://trust.exlibrisgroup.com/gdpr/ .
Position of the data protection officer	38	**Outline/Summary:** Article 38 stipulates the DPO's rights and the position within the organization of the controller and processor. **Ex Libris Statement:** Ex Libris has designated a data protection officer (DPO) position. Ex Libris will support the DPO in performing his/her tasks by providing the resources necessary to carry out those tasks and to maintain expert knowledge in accordance with the requirements of Article 38.
Tasks of the data protection officer	39	**Outline/Summary:** Article 39 stipulates the tasks and duties of the data protection officer (DPO). **Ex Libris Statement:** The Ex Libris DPO is involved with all aspects of data protection and is in a position to advise the company, monitor its compliance with the GDPR, and cooperate with the supervisory authority.
Codes of conduct	40	**Outline/Summary:** Article 40 allows for industry associations or bodies to create Codes of Conduct that specify the application of the GDPR in different areas.

		Ex Libris Statement: Currently there is no approved code of conduct for cloud-based SaaS providers. Ex Libris continues to monitor developments in the industry and will evaluate any applicable codes of conduct approved in the future by the European Commission.
Monitoring of approved codes of conduct	41	**Outline/Summary:** Article 41 provides that the monitoring of compliance with an approved code of conduct may be performed by an accredited industry association or body. **Ex Libris Statement:** Currently there is no approved code of conduct for cloud-based SaaS providers. Ex Libris continues to monitor developments in the industry and will evaluate any applicable codes of conduct approved in the future by the European Commission.
Certification & Certification Bodies	42 & 43	**Outline/Summary:** Articles 42 and 43 provide that the establishment of data protection certification mechanisms are to be encouraged for the purpose of demonstrating compliance with the GDPR. **Ex Libris Statement:** Currently there is no approved certification mechanism. Ex Libris continues to monitor developments in the industry and will evaluate any applicable certification mechanisms approved in the future by the European Commission. We note again that Ex Libris is certified as compliant with: • ISO 27001 standard (Information Security Management) - ISO 27001 is one of the most widely recognized, internationally accepted independent security standards. • ISO 27017 standard (Security Controls for Cloud Services) – ISO 27017 defines the code of practice for information security controls based on ISO/IEC 27002 for cloud services. • ISO 27018 standard (Cloud Privacy) - ISO 27018 is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Service. • ISO 22301 standard (Business Continuity) - ISO 22301 is a comprehensive standard that represents the highest level of commitment to business continuity and disaster preparedness.
Transfer of personal data to	44, 45, 46, 47,	**Outline/Summary:** Articles 44 to 49 of the GDPR stipulate the conditions for the international transfer of data to third countries.

third countries or international organizations	48, 49, 50	**Ex Libris Statement:** With respect to transfers of personal data to third countries outside of the European Union, Ex Libris ensures that such countries are recognized by the European Commission as providing an adequate level of data protection or that a mechanism is in place to provide appropriate safeguards and enforcement of personal data protection in compliance with the requirements of the GDPR.
Independent Supervisory Authorities	51, 52, 53, 54, 55, 56, 57, 58, 59	**Outline/Summary:** Articles 51 to 59 oblige member states to appoint independent public supervisory authorities responsible for the monitoring of the regulation. **Ex Libris Statement:** These articles are not applicable, as they apply only to supervisory authorities.
Cooperation and consistency	60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76	**Outline/Summary:** Articles 60 to 76 institute a European Data Protection Board which has the task of monitoring and ensuring the consistent application of the regulation and conducting reports regarding data protection. **Ex Libris Statement:** These articles are not applicable, as they apply only to the lead supervisory authority and the European Data Protection Board.
Remedies, liabilities, and penalties	77, 78, 79, 80, 81, 82, 83, 84	**Outline/Summary:** Articles 77 to 84 deal with remedies, liabilities, and sanctions. **Ex Libris Statement:** These are applicable to both controllers and processors.
Provisions relating to specific processing situations	85, 86, 87, 88, 89, 90 91	**Outline/Summary:** Articles 85 to 91 allow Member States to organize their own legislation in relation to freedom of information, public documents, and the collection of information for employment or scientific, statistical or historical purposes. **Ex Libris Statement:** Ex Libris shall comply with all laws and regulations applicable to its processing of personal data.
Delegated acts and implementing acts **&** **Final provisions**	92, 93, 94, 95, 96, 97, 98, 99	**Outline/Summary:** Articles 92 to 99 organize the entry into force of the regulation, and its relations with the already existing legal framework. **Ex Libris Statement:** Ex Libris is committed to supporting GDPR compliance across our products and services. We have closely analyzed the requirements of the GDPR, and our engineering, product,

		security and legal teams have worked to align our procedures, services, documentation, and contracts to support compliance with the GDPR. We continue to support customers in their GDPR compliance journey, using our strong foundation of certified security and data protection. Ex Libris understands that compliance is a shared responsibility with our customers, and we are committed to working with them to comply with the GDPR and future privacy requirements.

About Ex Libris

Ex Libris, a ProQuest company, is a leading global provider of cloud-based solutions that enable institutions and their individual users to create, manage, and share knowledge. In close collaboration with its customers and the broader community, Ex Libris develops creative solutions that increase library productivity, maximize the impact of research activities, enhance teaching and learning, and drive student mobile engagement. Ex Libris serves over 7,500 customers in 90 countries. Visit http://www.exlibrisgroup.com