



# Aurea Compliance Manager and GDPR Compliance

On 25 May 2018, the General Data Protection Regulation (GDPR) takes effect in the European Union (EU). The new regulation imposes broad new data privacy protections for EU individuals and applies to any company that collects or handles EU personal data, regardless of the company's location.

Aurea is committed to helping our customers comply with the GDPR through privacy and security protections in our products and services.

Below, we describe the steps we've taken to implement GDPR-compliant functionality in our Aurea® Compliance Manager (ACM) product, formerly known as NextDocs. Many of these features are already available; others will be available before the regulation takes effect.

## How Aurea Compliance Manager (ACM) Addresses GDPR Requirements

**Aurea is taking a multi-level approach to assist you with GDPR product compliance requirements, with minimal impact to customers:**

**Infrastructure** - Addressing core requirements around encryption, backups, and data retention.

**UI** - Addressing additional GDPR requirements through the user interface.

KEY GDPR REQUIREMENT	ACM CAPABILITIES
Encryption-at-rest of Personal Data	<ul style="list-style-type: none"> <li>For hosted installations, encryption-at-rest is already in place. Database files are encrypted and can only be read via the DBMS by the application or an administrator who has username and password credentials.</li> <li>On-premise customers are responsible for the security of their data; Aurea recommends enabling database encryption.</li> </ul>
Encryption-in-transit of Personal Data	<ul style="list-style-type: none"> <li>For hosted installations, ACM currently has encryption-in-transit in place, with the exception of the interface with AdLib. Encryption of data-in-transit for the AdLib interface will be added before the GDPR takes effect.</li> <li>For on-premise installations, Aurea recommends enabling encryption of in-transit data.</li> </ul>

## Infrastructure (cont'd)

KEY GDPR REQUIREMENT	ACM CAPABILITIES
Data Mapping / Data Inventory	<ul style="list-style-type: none"> <li>By default, ACM utilizes minimum personal data; name, user ID, and email address are the standard values. If the customer chooses to enable the SharePoint Profile feature, additional personal data can be stored in ACM.</li> <li>Customers are responsible for appropriate handling of any personal data contained in text documents. ACM can't systematically determine if such data is present, since the data is embedded in TextBlobs.</li> </ul>
Individual's Right - Data Retention	ACM does not provide self-service deletion capabilities. However, a user can request the removal of personal data and an administrator can delete the data.
Data Backups	<ul style="list-style-type: none"> <li>For our hosted customers, ACM keeps daily backups for 7 days and weekly backups for 7 weeks.</li> <li>For on-premise installations, the data retention period for backups is configured by the customer. We recommend that the customer consider GDPR concerns when determining this value.</li> </ul>
Privacy by Design	ACM is updating its development processes to include data privacy reviews during architecture, design, implementation, and testing.

## User Interface

The features listed below are already provided in currently supported versions of Aurea Compliance Manager.

KEY GDPR REQUIREMENT	AUREA CAPABILITIES
Individual's Right to Access and Review	<ul style="list-style-type: none"> <li>By default, the only personal data that ACM stores is name, user ID, and email address. The user cannot see this information.</li> <li>The SharePoint Profile feature can provide the user with the ability to view their data. The feature is not utilized by ACM by default.</li> </ul>
Individual's Right to Update Data	<ul style="list-style-type: none"> <li>By default, the only personal data that ACM stores is name, user ID, and email address. The user cannot see and edit this information. A system administrator can update the email address when required; editing of the user ID is not permitted.</li> <li>The SharePoint Profile feature can provide the user with the ability to edit their data. The feature is not utilized by ACM by default.</li> </ul>
Individual's Right - Data Portability	Since only the name, user ID, and email address are stored in ACM, the data portability standard does not apply.
Individual's Right - Commonly Used Format	Since only the name, user ID, and email address are stored in ACM, the commonly used format standard does not apply.
Individual's Right to Erasure	A user can be deleted and data removed upon the user's request. Permission to do so may be restricted to an administrator.
Individual's Right - Consent	ACM users are employees or agents of our customers. It is the customer's responsibility to obtain consent from its employees (or agents) if consent is required under the applicable laws.
Cookies Consent	SharePoint requires cookies. We will be adding a consent notice to versions 5, 6.1, and 6.2 to notify users that ACM uses cookies.

# Platinum Data Protect Services

Aurea is also offering a series of services, for cloud and hosted customers, to improve your flexibility and ease of GDPR compliance.

The following table describes additional GDPR-related services that you may access as part of your Aurea Platinum Support subscription.

SERVICE	DESCRIPTION
Individual's Right - Data Portability: Quick Download	<b>Cloud and Hosted Solutions</b> <ul style="list-style-type: none"><li>Aurea will create a file containing the user's profile information.</li><li>This allows you to quickly access and manage the information you provide to your users upon their requests for data portability.</li></ul>
Individual's Right to Erasure: Delete	<b>Cloud and Hosted Solutions</b> <p>Aurea will clear a user's profile data. The user's information will not be removed from the audit data.</p>

Aurea Platinum Support customers may submit a ticket through the Customer Support Portal at any time to request these services be performed. We estimate that the request will take two weeks to be resolved.

## We're Here to Help

If you have any additional questions or need assistance, please contact support. Aurea's Professional Services team is also available to assist with special customizations or configuration needed to assist you with product GDPR compliance; for more information please contact your account manager.

### Legal Notices

Copyright © 2018. Aurea Software, GmbH. All Rights Reserved. These materials and all Aurea products are copyrighted and all rights are reserved by Aurea. Aurea and design are registered trademarks of Aurea. Additional Aurea trademarks or registered trademarks are available at: <http://www.aurea.com/legal>. All other marks contained herein are for informational purposes only and may be trademarks of their respective owners.

The information in these materials is for informational purposes only and Aurea and its affiliates assume no responsibility for any errors that may appear herein. Aurea reserves the right to revise this information and to make changes from time to time to the content hereof without obligation of Aurea to notify any person of such revisions or changes. AUREA MAKES NO EXPRESS GUARANTEES OR ANY GUARANTEES IMPLYING LEGAL INTENT WITHIN THIS DOCUMENT. The content of this document is not intended to represent any recommendation on the part of Aurea. Please consult your legal and compliance advisors to confirm that your use of this document is appropriate, that it contains the appropriate disclosures for your business, and is appropriate for the intended use and audience.

This document may provide access to or information on content, products, or services from third parties. Aurea is not responsible for third party content referenced herein or for any changes or updates to such third party sites, and you bear all risks associated with the access to, and use of, such web sites and third party content. Aurea and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

