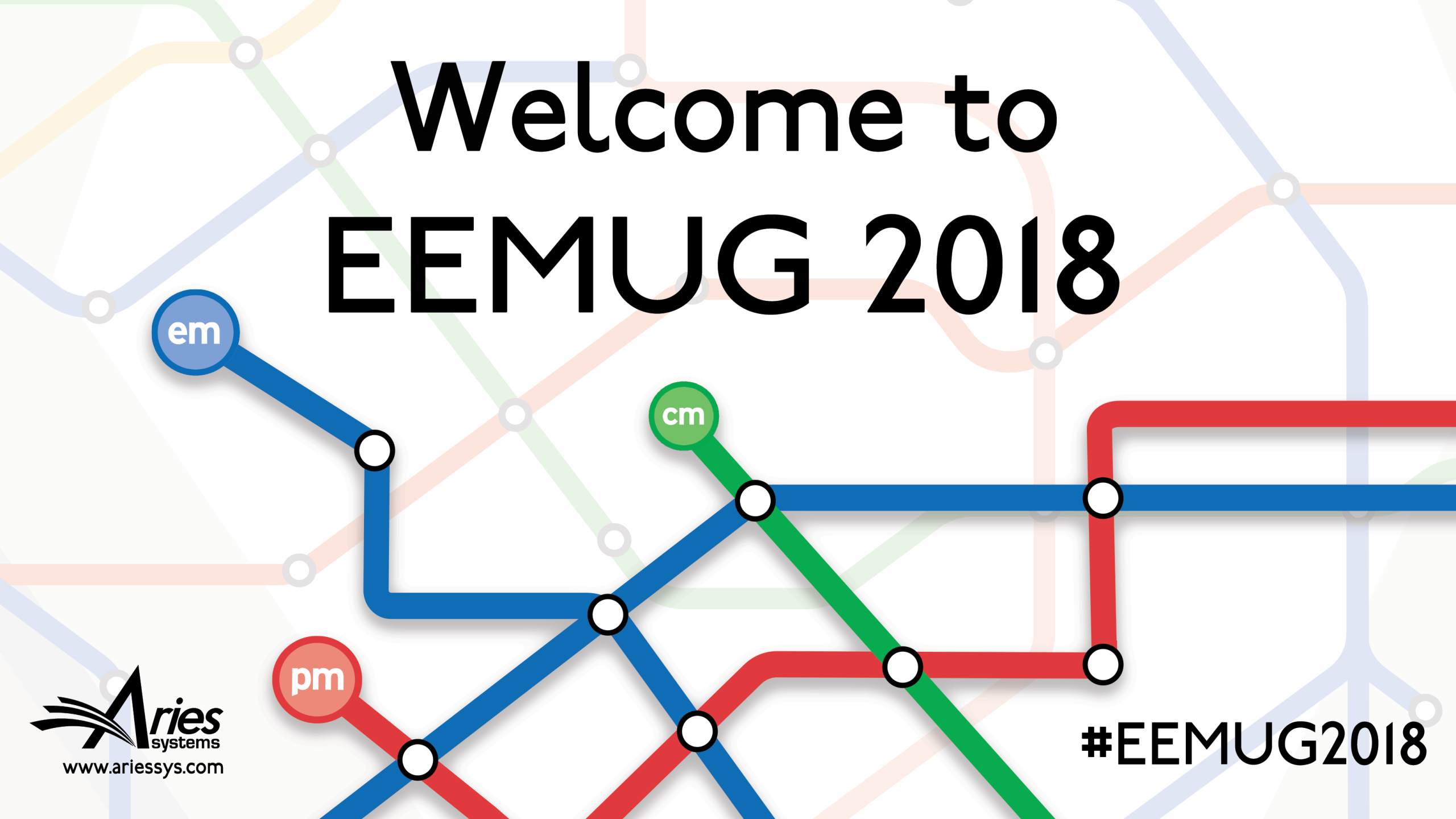
Welcome to EEMUG 2018



Aries systems
www.ariessys.com

#EEMUG2018

EU General Data Protection Regulation

Sally Ubnoske, Senior Business Systems Analyst, subnoske@ariessys.com

Sean MacRae, Business Systems Analyst, smacrae@ariessys.com

GDPR Summary

- The European Parliament, the European Council, and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU)
- It also addresses the export of personal data outside of the EU
- The primary objective is to return control of personal data to citizens and to simplify the regulatory environment of international business
- It applies to any entity processing data about EU residents, wherever that entity is located in the world

Data Controller vs. Data Processor

- Data Controller – the entity that determines the purposes, conditions, and means of processing personal data
- Data Processor – processes personal data on behalf of the Data Controller
- Under these terms,
  - The **Publisher, Society, or Journal** is the *Data Controller* (Journal staff implement Data Controller policies)
  - **Aries Systems Corporation** is a *Data Processor*

Key Changes vs. Data Protection Directive

- Applies to all companies processing personal data of EU residents regardless of the company's location
- Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 million (whichever is greater)
- Conditions of consent have been strengthened – companies can no longer use illegible terms and conditions full of legalese
- Consent must be clear and distinguishable and provided in clear and easily accessible form
- Consent must be as easy to withdraw as to give

Personal vs. Sensitive Personal Data

- Personal Data
  - Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier
- Sensitive Personal Data
  - The special categories include medical or genetic data, and biometric data where processed to uniquely identify an individual
  - Additional safeguards are required for such data

Personal Data Must Be . . .

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed
- Processed in a manner that ensures appropriate security of the personal data using appropriate technical or organizational measures (Aries, as Data Processor, provides this while in EM)

Data Subject Rights

- Right to Access
- Clear Consent
- Right to be Forgotten
- Data Portability
- Privacy by Design
- Data Protection Officers
- Breach Notification

Right to Access

- Data subjects have the right to obtain confirmation from the Data Controller as to whether personal data about them is being processed, where, and for what purpose
- The Data Controller shall provide a copy of the personal data, free of charge, in an electronic format
  - GDE and reports allow this via tab-delimited text formats
- This is a dramatic shift to data transparency and empowerment of data subjects

Clear Consent

- Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her
- Consent can be given by a written statement, including by electronic means, or an oral statement. This may include ticking a box when visiting an internet website
- The data subject shall have the right to withdraw his or her consent at any time. It shall be as easy to withdraw consent as to give it.

Right to be Forgotten

- Also known as ‘Data Erasure’
- Entitles the data subject to have the data controller erase or anonymize his/her personal data and cease further dissemination of the data
- May require that third parties halt processing of the data
- The conditions (per Article 17) include that the data is no longer relevant to its original purpose if a data subject withdraws consent
- Data Controllers are required to compare data subjects’ rights to the public interest in the availability of the data
    - Author and Reviewer details may need to be retained for use in potential scientific fraud cases

Data Portability

- Data subjects have the right to receive the personal data concerning them in a commonly used and machine readable format
- Data subjects have the right to transmit their personal data to another Data Controller

Privacy by Design

- Privacy by Design has existed as a concept for years but is only now part of a legal requirement with the GDPR
- It calls for the inclusion of data protection from the onset of designing systems, rather than as an addition
- Per Article 23, the Data Controller can hold and process only the data that is absolutely necessary for the completion of its duties
- Access to personal data is limited to those needing to perform the processing.
  - This is handled via *RoleManager* permissions that limit Editor access to assigned submissions only, Reviewer blinding, etc.

Data Protection Officers

- The appointment of a Data Protection Office (DPO) is mandatory when monitoring data subjects on a large scale or of special categories of data, i.e. criminal offenses
- The DPO must have expert knowledge on data protection law and practices
- The DPO may be a staff member or external service provider
- They must be provided with appropriate resources
- They must report directly to the highest level of management
- They must not carry out other tasks that result in a conflict of interest

Breach Notification

- Mandatory where breach is likely to result in a risk for the rights and freedoms of individuals
- Notification to the data subjects must come within 72 hours of first becoming aware of the breach
- Data Processors must notify their customers, the Data Controllers, without undue delay

How does EM support Publishers with the GDPR?

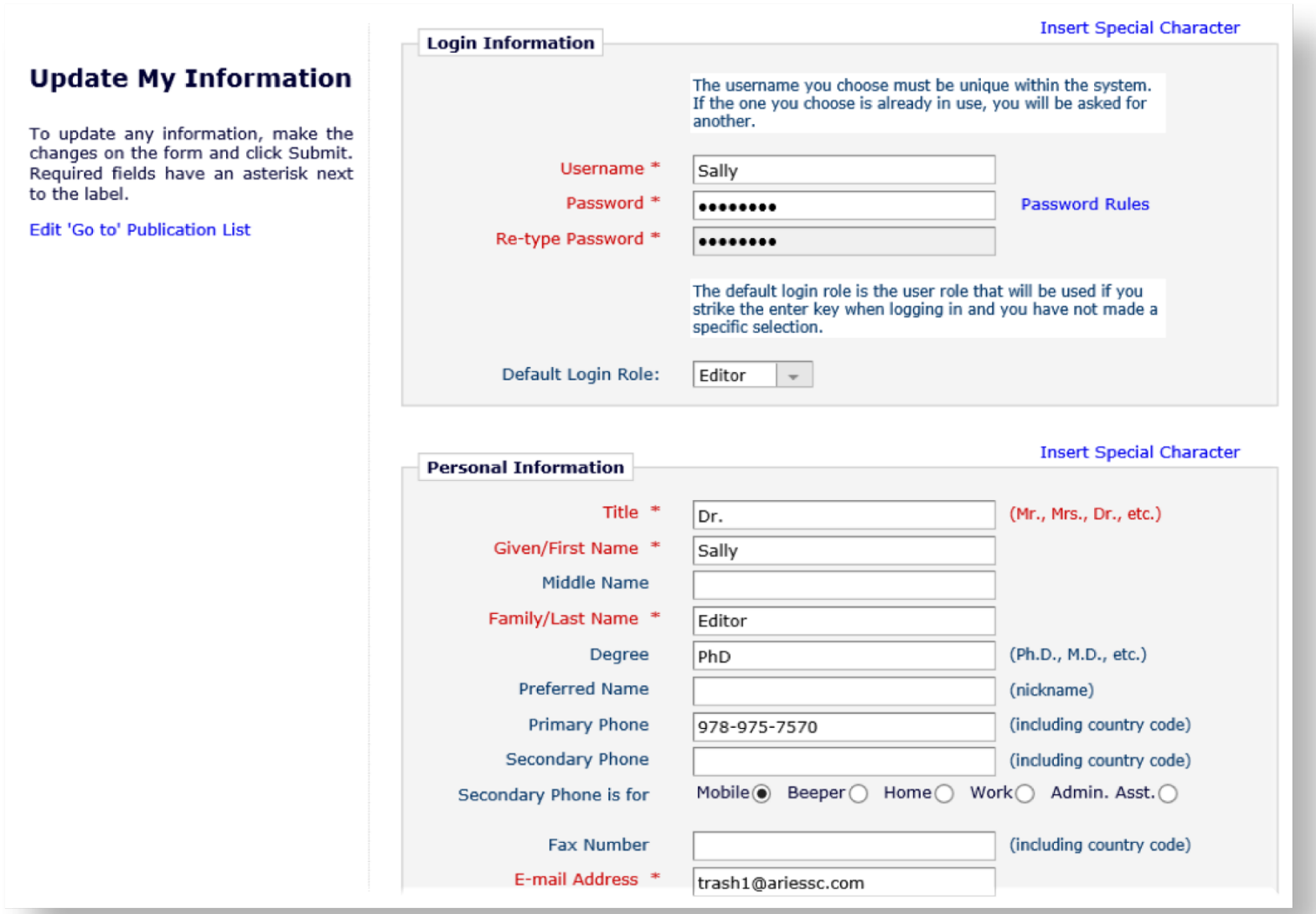
Key Existing Design Features

- Existing design restricts access appropriately by Role
- Use Role permissions to restrict access to personal data to appropriate users
  - Restrict View and Edit People permissions
  - Restrict Search People
  - Restrict View All Submissions, use Search Only Assigned Submissions
- GDE and Custom Reports allow export to CSV – a common interchange format (Data Portability)
- Reporting Permissions are broad
  - Restrict to key personnel
- Publishers can restrict admin rights

Consent and Right to Access

- Users typically choose to self-register on an Editorial Manager site
- Aries is implementing functionality to prevent users from being proxy-registered without being notified
  - This functionality applies where the proxy-registration is likely to be the point-of-entry into the Publisher's systems
- Users can view their people-related information at any time, by logging into an EM site

Right to Access – 'Update My Information'



Update My Information

To update any information, make the changes on the form and click Submit. Required fields have an asterisk next to the label.

Edit 'Go to' Publication List

Insert Special Character

Login Information

The username you choose must be unique within the system. If the one you choose is already in use, you will be asked for another.

Username * Sally

Password * ••••••••

Re-type Password * ••••••••

Password Rules

The default login role is the user role that will be used if you strike the enter key when logging in and you have not made a specific selection.

Default Login Role: Editor

Insert Special Character

Personal Information

Title * Dr. (Mr., Mrs., Dr., etc.)

Given/First Name * Sally

Middle Name

Family/Last Name * Editor

Degree PhD (Ph.D., M.D., etc.)

Preferred Name (nickname)

Primary Phone 978-975-7570 (including country code)

Secondary Phone (including country code)

Secondary Phone is for Mobile ◉ Beeper ○ Home ○ Work ○ Admin. Asst. ○

Fax Number (including country code)

E-mail Address * trash1@ariessc.com

Consent – New Forced Registration Question

- New ‘Forced’ Registration question to confirm that users have reviewed the Privacy and Data Use Policies from the Publisher and Aries
- When users agree to the question, the date/time and IP address is stored in their People table record

Consent – Proxy Registration

- Users need to be notified when they have been registered in EM
- Currently, new users can be proxy registered in one of the following ways:
  - Proxy Register New User
  - Register and Select New Reviewer
  - Register and Invite New Author
  - Reviewer Discovery
  - EM-to-EM Submission Transfer for publications that are not in a People Sharing Group

Mandatory Notification of Proxy Registration

New proxy registration restrictions are enabled at upgrade to version15.0:

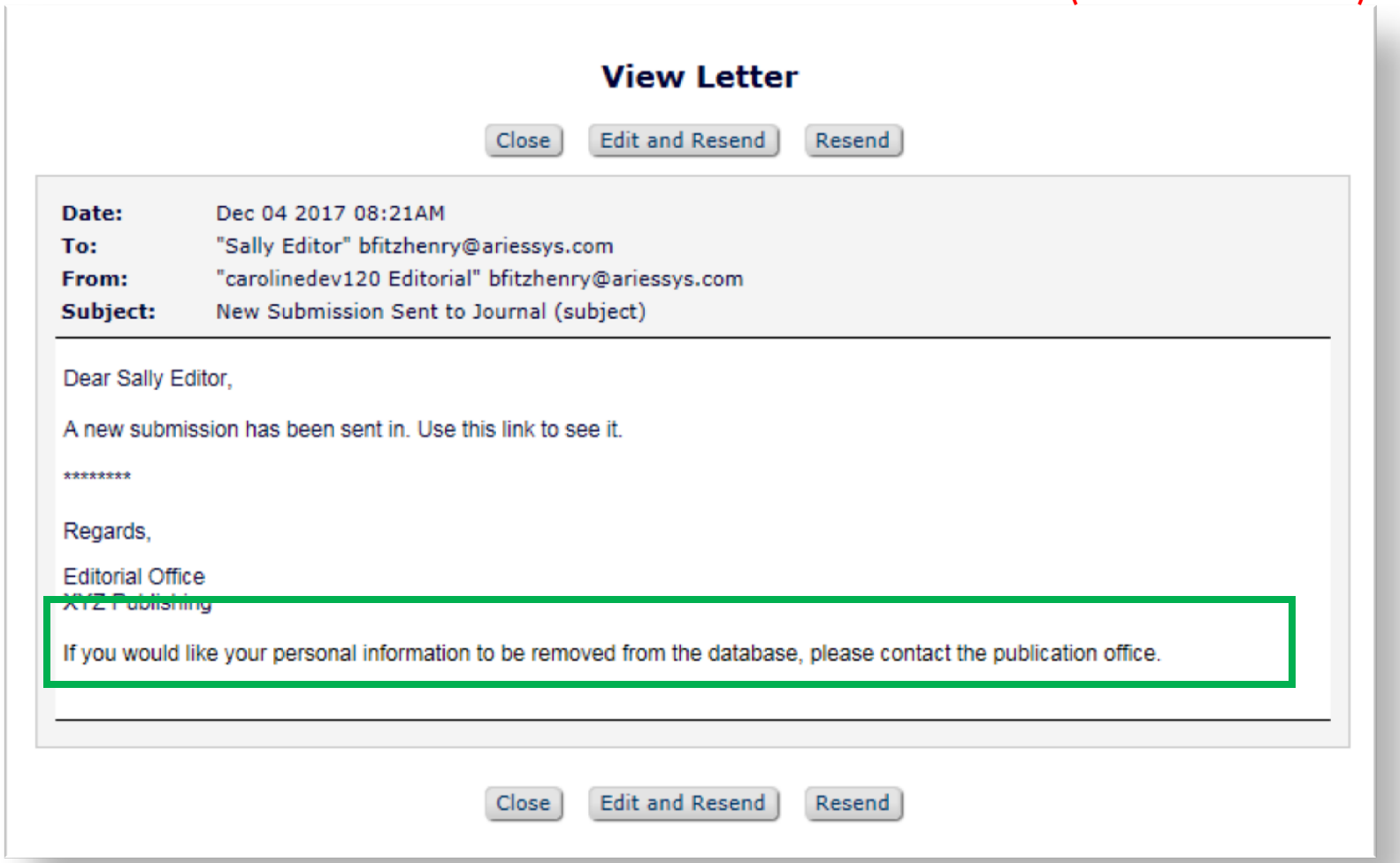
- The ‘Register User and Do NOT Send Letter’ button is suppressed and the Editor must enter an email address
- The new user is proxy registered but is set to ‘INACTIVE’ until the ‘Proxy Register New User’ letter is sent
- The proxy registered user’s record is deleted during the nightly Batch job if they are still ‘INACTIVE’, i.e. have not been sent a letter
- Proxy registration that occurs for Reviewer Discovery sends the ‘Proxy Register New User’ letter. If the candidate does not have an email address, they cannot be selected as a Reviewer

Right to be Forgotten / Data Erasure

- New footer text will be added to all letters sent from EM/PM/CM in version 15.0
- The footer will direct users to contact the Journal Office if they wish to request that their information be removed / anonymized
  - Aries will provide guidance regarding the steps to anonymize the user's data
- Additional functionality will be added in version 15.1 to include an embedded hyperlink in the footer
- Clicking the link will send a letter to the journal office to notify them of the user's request to be removed.
  - The journal office will see a new button on the *Search People – Update Information* page
  - Clicking the new button will anonymize the user's data. An option to retain the user's Given Name and Surname will be available for cases where the user's Reviewer or Editor Roles are still relevant

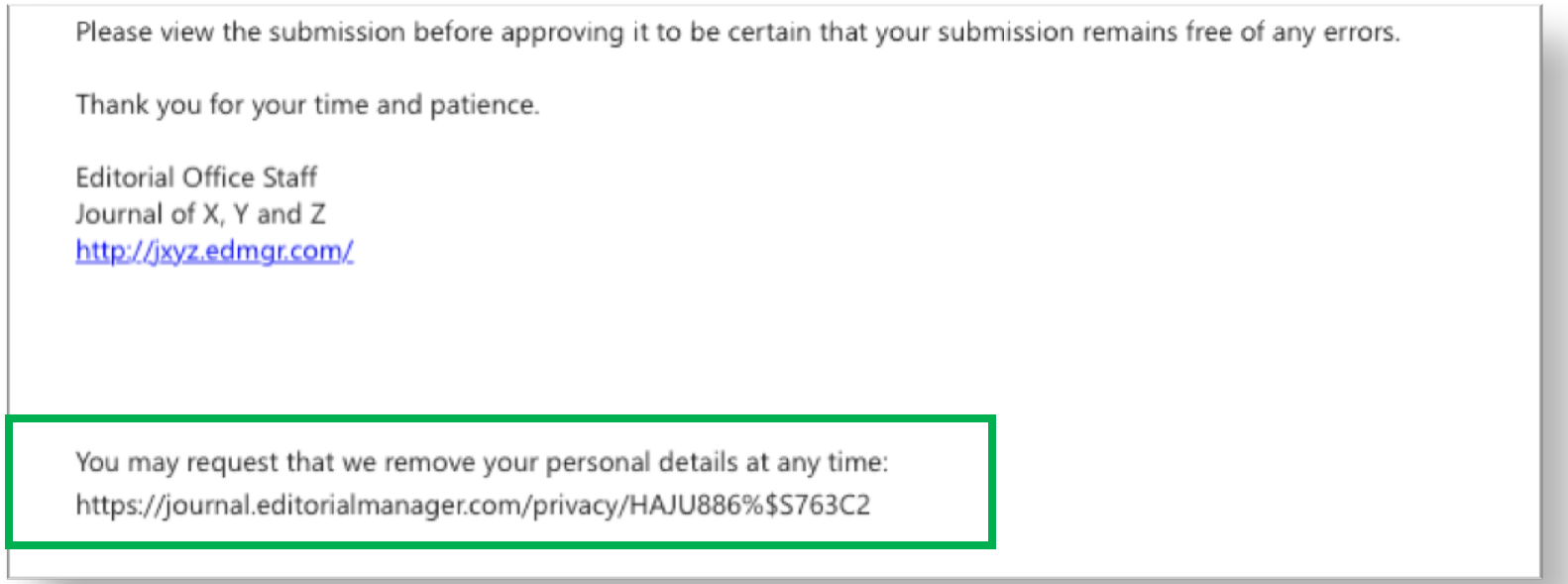
Right to be Forgotten / Data Erasure

(EM Version 15.0)



Right to be Forgotten / Data Erasure

(EM Version 15.1)



Please view the submission before approving it to be certain that your submission remains free of any errors.

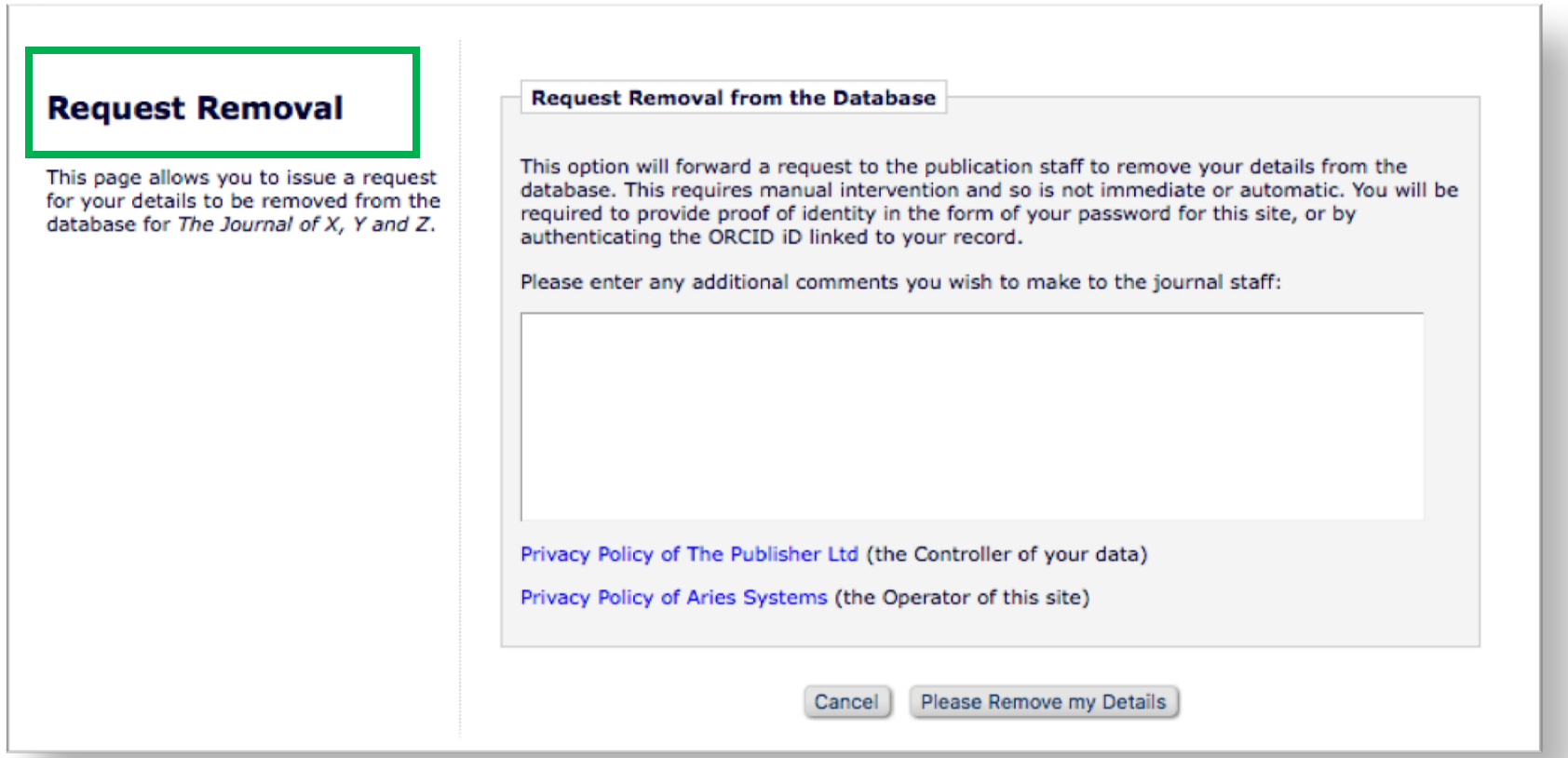
Thank you for your time and patience.

Editorial Office Staff
Journal of X, Y and Z
http://jxyz.edmgr.com/

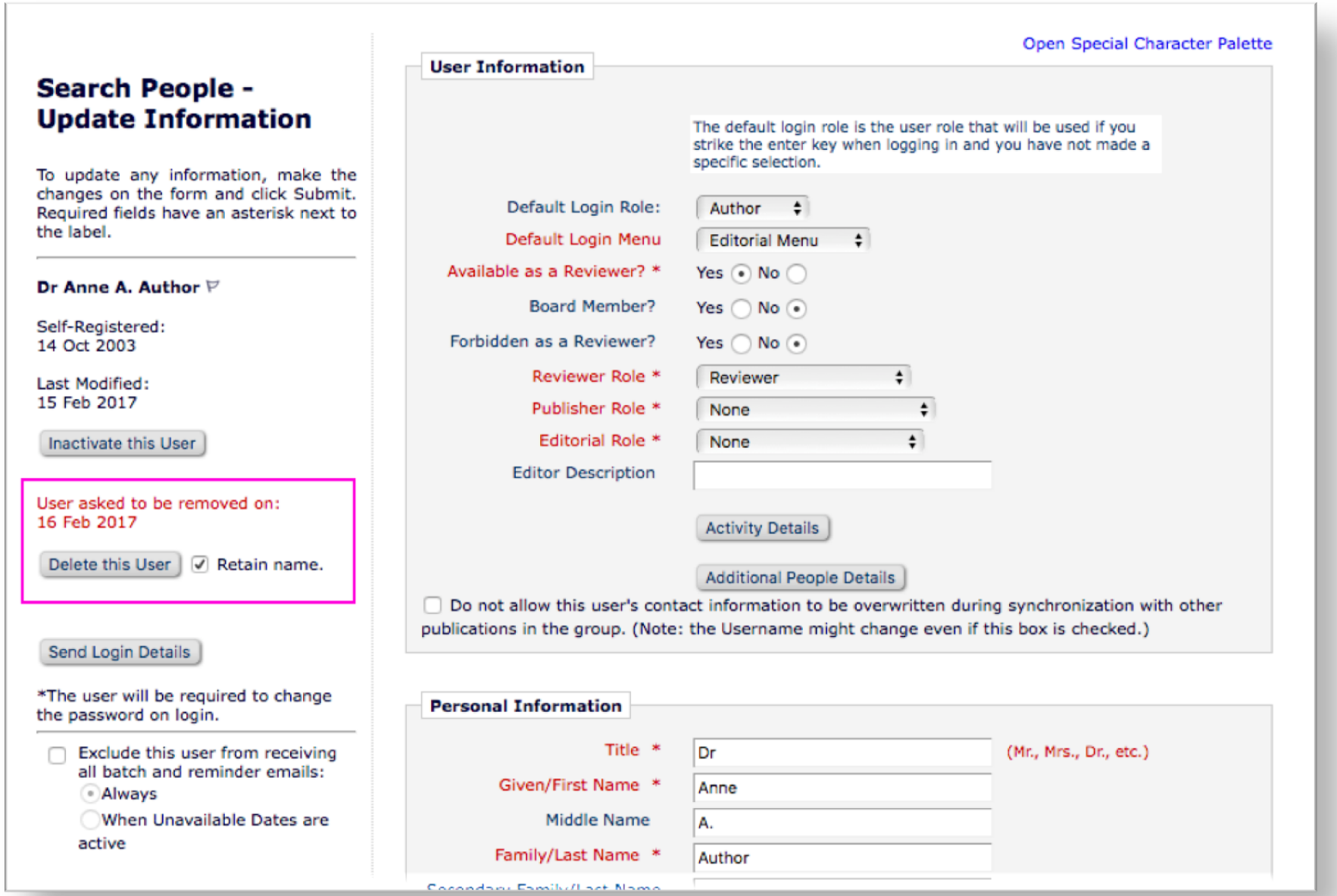
You may request that we remove your personal details at any time:
https://journal.editorialmanager.com/privacy/HAJU886%$S763C2

Right to be Forgotten / Data Erasure

(EM Version 15.1)



(EM Version 15.1)



Search People - Update Information

To update any information, make the changes on the form and click Submit. Required fields have an asterisk next to the label.

Dr Anne A. Author

Self-Registered:
14 Oct 2003

Last Modified:
15 Feb 2017

Inactivate this User

User asked to be removed on:
16 Feb 2017

Delete this User ☑ Retain name.

Send Login Details

*The user will be required to change the password on login.

☐ Exclude this user from receiving all batch and reminder emails:
- ◉ Always
- ○ When Unavailable Dates are active

Open Special Character Palette

User Information

The default login role is the user role that will be used if you strike the enter key when logging in and you have not made a specific selection.

Default Login Role:	Author
Default Login Menu *	Editorial Menu
Available as a Reviewer? *	Yes ◉ No ○
Board Member?	Yes ○ No ◉
Forbidden as a Reviewer?	Yes ○ No ◉
Reviewer Role *	Reviewer
Publisher Role *	None
Editorial Role *	None
Editor Description	

Activity Details

Additional People Details

☐ Do not allow this user's contact information to be overwritten during synchronization with other publications in the group. (Note: the Username might change even if this box is checked.)

Personal Information

Title *	Dr	(Mr., Mrs., Dr., etc.)
Given/First Name *	Anne	
Middle Name	A.	
Family/Last Name *	Author	

EM and GDPR Compliance

Right to Access/Data Portability	EM users can access their information at any time by logging into a site where they are registered. Admins can supply data via GDE
Clear Consent	Mandatory Registration Question Can no longer be proxy-registered without notification
Right to be Forgotten	New footer text is added to all EM emails 15.0 – users contact the JO and information is anonymized manually 15.1 – users click link and the JO clicks button to anonymize automatically

EM and GDPR Compliance

Privacy by Design	Aries' development follows best practices with regard to data protection and privacy
Data Protection Officer	Aries Data Protection Officer can be reached by sending an email to privacyofficer@ariessys.com
Breach Notification	In the event of a detected data breach, Aries Client Services will notify Publishers

Why wait?

- Aries can already turn on enforced proxy notifications for individual journals
- You can set up your own Forced/Required Registration Questions for consent
- You can set up a Custom Merge Code to insert instructions/contacts for requesting removal
- You could consider restricting the ability to proxy register new reviewers
- You should review Editor permissions, considering who should be able to:
  - View every submission in the system
  - Search the entire people database
  - Generate reports and potentially export bulk data

What are the Publisher's Responsibilities?

Publisher Responsibilities

- Data Use and Privacy Policy
  - EM will include links to the Data Controller's Data Use and Privacy Policy; this is your opportunity to explain how user data will be used/transferred during the publishing process
  - Publishers must provide Aries with a URL/URI for their Data Use and Privacy Policy
- Data Loads
  - Publishers and/or Journals are responsible for notifying data subjects that they have been registered via a Data Load
- Data Protection Officer
  - Larger Publishers may need to identify a Data Protection Officer
  - The Publisher must notify Aries of the DPOs Contact Details (in the event of a data breach)

Questions

- Publishers are encouraged to contact their appropriate legal representatives with any questions or concerns
- Aries Systems Corporation does not represent its interpretation of GDPR requirements as being definitive with respect to the Data Controller's obligations under the GDPR.


THANK YOU
Maake
Ua Tsaug Rau Koj
Mochchakkeram
Terma Kasih
Merci
Juspaxar
Chokran
Mauna
Kiitos
Grazie
Asante
Matondo
Dank Je
Merci
Obrigado
Multumesc
Spasibo
Nirringrazzjak
Matondo
Salamat
Matur Nuwun
Chokrane
Arigato
Obrigado
Welalin
Multumesc
Kiitos
Merci
Mochchakkeram
Chokrane