Record audit trail GDPR compliance requirements

Problem

Europe’s GDPR requires information systems to handle personally identifying information in a variety of ways, including barring associating specific users with specific acts in that system, as well as ensuring the “right to be forgotten”. In order for FOLIO to be fully adopted in EU countries, FOLIO needs to comply with these regulations.

Currently, FOLIO tracks when a record was created and last updated and provides the “source” as the logins of the users who made the entries and/or edits.

Additionally, FOLIO provides a more comprehensive record audit trail for Orders and PO Lines, and is expected to extend this functionality to additional record types in upcoming releases.

For EU libraries using individual logins, this is a potential showstopper.

Current workarounds

EU libraries using FOLIO are currently working around this restriction via shared or functional logins rather than individual logins.

Use cases

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Status</th>
<th>Use case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optionally disable capture of “Source” in record details and version histories</td>
<td>VERIFIED</td>
<td>Supervisors and administrators must be unable to associate a particular staff member with a particular action in FOLIO.</td>
</tr>
<tr>
<td>Audit trail must be configurable</td>
<td>VERIFIED</td>
<td>Libraries not subject to GDPR should have the option of associating specific staff with specific actions</td>
</tr>
<tr>
<td>Disabled Source must not be retained anywhere in the system</td>
<td>VERIFIED</td>
<td>System administrators must not be able to reconnect hidden or masked user information to particular actions in FOLIO</td>
</tr>
<tr>
<td>Deleted/disassociated staff member should leave no identifiable artifacts in the system</td>
<td>PENDING</td>
<td>Right to be forgotten requires all identifying information be purged from the system on demand.</td>
</tr>
</tbody>
</table>

Questions
Is it OK to mask/hide or is the requirement not to collect? - **Do not collect.** Back end collection is still technically reportable, which some institutions view as a GDPR violation (GDPR verbiage is not entirely clear).

**Proposed approach(es)**

- Enable/disable "source" collection at the Tenant level (applies to all records across the entire tenant)
- App-based approach (enable/disable on a per-app basis)

**Additional info**

- GDPR permits collection of PII but restricts how it can be used
- Privacy SIG
- This is a cross-app issue