

Audited Delete

! Audited Delete Allows You to:

- Comply with the EU GDPR 'Right to be Forgotten'
- Construct a full, transparent audit trail documenting the process of deletion
- Ensure a minimum of two nominated users check any items for deletion
- Note a reason and record for any deleted emails for future reference

! Audited allows you to

As our customers began to prepare for EU GDPR we recognised the need to introduce a delete functionality that matches the Cryoserver compliance-first mentality. If your users send sensitive information which should not be held for longer than it is needed, this functionality will help.

We ensure that two separate internal officers at every customer organisation have eyes on every single deletion, allowing your business to only ever delete emails which need to be deleted. Not only that, but we've built in a variety of fail-safes, which prevent any accidental deletion if users take reasonable care.

! Keeping Cryoserver Compliant

The compliance element of Cryoserver is critical to the product. At its heart Cryoserver has always enabled businesses to exist within the toughest requirements of their industry. By ensuring that any deletion is accompanied by an audit trail including reasoning as well as multiple approvals.

Our new Audited Delete function creates the same forensic audit trail which has been used time and again in court to demonstrate fair searches.

Audited Delete

! Keeping Cryoserver Compliant

On rare occasions, there may be a need to delete email(s) from the

Cryoserver repository and to help maintain the high compliance and evidential repository, Cryoserver have developed a four eye methodology to control the process of destruction of data from the repository. It involves two roles working in collaboration and independently to initiate and control the deletion.

Privileged User

Cryoserver Privileged Users will identify email(s) to be deleted from the repository via the familiar search interfaces. Once identified these searches / emails are shared with the Cryoserver Privileged and Delete User. Prior to sharing the Privileged user is presented a reconfirmation message to initiate the start of the deletion process and empowering the Privileged & Delete User with entitlement to delete the email.

Request for Deletion

Privileged Delete User

Once reviewed, the Privileged & Delete User is able to Approve the deletion request or Decline via Action Icons and a check box selection. If approved secondary warning is presented to the user asking for confirmation for deletion.

Once approved both users are informed the Deletion Request has been approved – this is considered the 3rd and final warnings.

At the defined deletion time, the email(s) will be expunged from the system and Audit trails are presented to the users confirming the deletion(s) have been completed. The Audit trails can be used as certificates to share with the Data Subjects who desire the Right to be forgotten requests.

Furthermore, Data Guardian Users are overseeing the entire process and will be informed of each of the steps.

To enable the Privileged & Delete User Role on your Cryoserver please contact Cryoserver Support on support@cryoserver.com

