Datasheet

Audited Delete

Cryoserver™

"The audit trail is particularly useful... It allows us to manage our staff fairly"

David Chatterton, ICT Infrastructure Specialist, South Liverpool Homes

For effective management of sensitive data

Thanks to GDPR, organisations now have to deal much more carefully with the personal identifiable information they hold on their systems. And they need to be ready to carry out Right to be Forgotten requests. That's what Cryoserver's Audited Delete function is for. It enables users to effortlessly find and delete relevant customer data quickly from the archive and users' mailboxes.

Unlike other email archiving solutions, Cryoserver provides audit trails of the request, recording who approved it and confirming that the relevant data was deleted. These trails act as certificates which you can pass back to the data subject to prove the deletion was successful.

Benefits

- 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 dele-tion
- Record a reason for any deleted emails for future reference

If your users send sensitive information which should not be held for longer than it is needed, Audited Delete will help you.

Overseeing deletions

We ensure that two separate internal officers at your organisation have eyes on every single deletion. This way your business only ever deletes emails which need to be deleted. Also, 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 meet the toughest regulations of their industry. We do this by ensuring that any deletion is accompanied by an audit trail including reasoning as well as multiple approvals. Our Audited Delete function creates the same the same type of forensic audit used in courts to demonstrate fair searches.

How to control deletion of emails

On rare occasions, your organisation may need to delete (an) email(s) from your Cryoserver repository. To help maintain the high compliance and evidential archive, we've developed a rigorous oversight methodology to control the process of destruction of data from the repository. It involves two people with different roles, working in collaboration and independently, to initiate and control the deletion. We call these two the Privileged User and the Privileged & Delete User. A third person, your appointed Data Guardian, oversees the actions of the other two.

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

Once the Privileged & Delete User reviews the email(s), they can either Approve the

deletion request or Decline via Action Icons and a check-box selection. If the request is approved, a secondary warning is presented to the user asking for confirmation for deletion. Once this is done, both users are informed the Deletion Request has been approved – this is considered the third and final warning.
At the defined deletion time, the email(s) will be expunged from the system and Audit trails presented to the users confirming the deletion(s) has / have been completed. The Audit trails can be used as certificates to share with the Data Subjects who made the Right to be forgotten requests.

The Data Guardian will be overseeing the entire process and will be informed of each of the steps.

To enable the Privileged & Delete User role on your Cryoserver, please email us at support@cryoserver.com