arcserve®

WHITE PAPER

Arcserve UDP Archiving Technical Whitepaper

Preparing for the General Data Protection Regulation (GDPR)

The European Union (EU) General Data Protection Regulation (GDPR) is one of the most demanding compliance mandates to date, aimed at ensuring that any organization working with European consumers or enterprises use all the necessary means to protect the personal data of individuals.

With the May 25, 2018 deadline fast approaching, organizations need to focus on one of their most essential and mission-critical applications—email—to ensure they meet a key principle of the legislation: accountability. Given that more than 60 billion emails are created every day and they represent a vital part of every business, the potential for compliance violations is substantial.

What is personal data?

Personal data includes the fairly obvious email addresses, names, telephone numbers and location information that can identify an individual. In addition, other identifiers such as IP address, for example, are also included in the scope of the regulation, making it very broad.

Defined in Article 4, "personal data" is "any information relating to an identified or identifiable natural person … who can be identified, directly or indirectly … by reference to an identifier." Identifiers listed in Article 4 include name, identification number, location data, and other identifying factors, such as physical, mental, and cultural, among others.

The magnitude of fines set in Article 83 for non-compliance and breaches are tough, with €20 million, or 4% of global revenue, under the GDPR.

Specific compliance challenges for email

Personal data about individuals is shared extensively within emails, and these emails must be produced by an organization if a subject access request (SAR) is made by individuals exercising their right to see their personal data. Considering the daily volume of emails, and the fact that some sectors must retain emails for many years, the GDPR will have a huge impact on how emails are processed, archived, and accessed in relation to ease of accessibility in the event of a SAR. Such requests must be fulfilled within 30 days, and at no cost to the individual.

The number of SARs is set to increase, but IT managers can't afford to have their time taken up with these requests. This administrative burden can be handled only by effective technical solutions and business processes.

Non-compliance can be costly in fines, reputation, and loss of customers

With fines as high as 4% of global revenue, GDPR cannot be ignored by any organization.

In this digital age, reputations can live or die on social media. And with competitors only one click away, organizations cannot afford to risk the long-term fallout of lost business because customers are concerned that adequate procedures aren't being followed to secure their personal data.

People must be informed if their data is stolen in a cyberattack, and they can sue. Awareness of these rights is growing, and such action is inevitable if customers believe their data has been mishandled or compromised by an organization.

Solutions for managing emails under GDPR

The critical first step in complying with GDPR is gaining a holistic understanding of the location of all personal data held by an organization. Email records, specifically, must be contained in an unalterable archive with set policies to automate the management process. Further, organizations must be able to quickly and easily respond to SARs, perform the "right to be forgotten" process, and manage email records with collection policies such as time to retain, exceptions from archiving, and end of life purging.

Arcserve offers powerful, compliance-driven email archiving technology designed to protect corporate email records and make them easily accessible for regulatory compliance, legal discovery, and corporate governance with seamless access for employees.

Arcserve UDP Archiving for GDPR Compliance

Arcserve UDP Archiving is a purpose-built, multi-tenant capable solution that supports on-premises, private and public clouds – ready for your network or managed as a cloud service. It treats every collected email as an unalterable corporate record, managed through the following steps:

Collection

Efficiently collects all new emails in real-time as they are sent or received with the ability to archive all historical messages from your mail server or prior archive system.

Apply Policies

Automatically applies policies such as message retention, exceptions, or legal holds based on employees, domains, or content.

Full text Index

Full text index of every message and attached for fast, accurate searches.

Encryption

Every message is stored as a protected, encrypted file to meet privacy and data protection laws.

Protected Access

Strong controls to restrict access to only users with authority to meet privacy and security requirements. Only designated Auditors can access company email records.

Compression & Single Instance Storage

Data is compressed and stored with single instance storage which represents big storage cost savings.

Disposition

At the end of a messages retention period, unless there is a legal hold in place, messages are systematically removed.

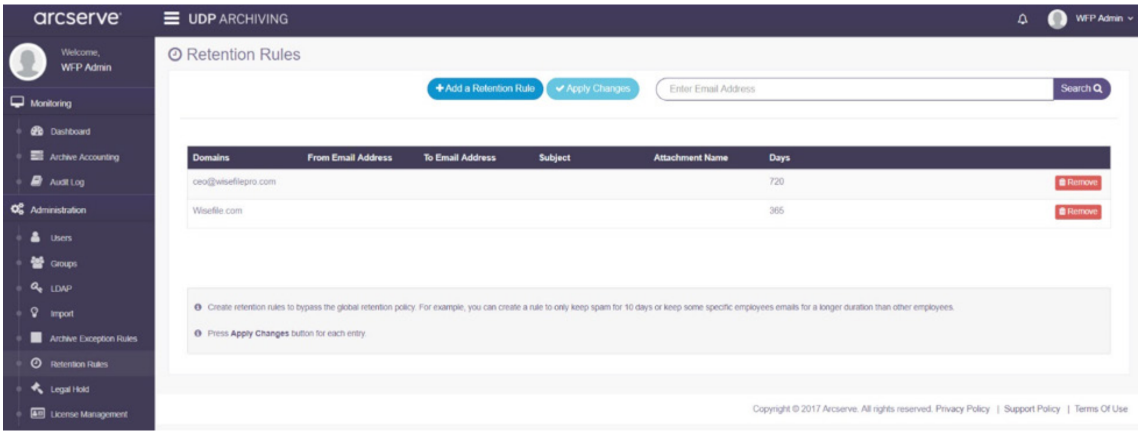
Built with Data Protection Officers in Mind

UDP Archiving has a dedicated role for the Data Protection Officer (DPO) to manage the GDPR process. This specific role has the ability to access the archive and view all email records, set policies, perform steps for Subject Access Requests (SAR) and maintain proactive and reactive control of the data.

Policy Management

Automated management of corporate policies is easy, and can be modified whenever needed as policies may change.

- **Retention**
  Setting policies that define how long a message should be held is a critical function for complying with GDPR. The DPO can easily manage email records to a useful life, and at the end of the retention period, purge them from the archive. Further, the DPO can modify a records policy to adhere to a "right to be forgotten" request. Retention policies can be set based on:
  - Company domain(s)
  - Email address – sender or receiver
  - Email subject line
  - Message size
  - Attached file name



Domains	From Email Address	To Email Address	Subject	Attachment Name	Days
ceo@wisefilepro.com					720
Wisefile.com					365

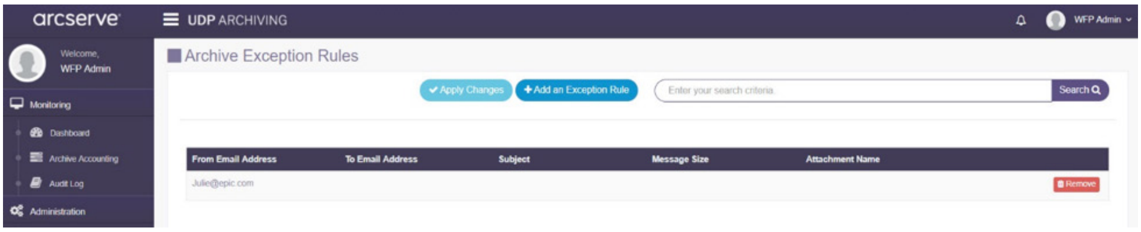
Create retention rules to bypass the global retention policy. For example, you can create a rule to only keep spam for 10 days or keep some specific employees emails for a longer duration than other employees.

Press **Apply Changes** button for each entry.

Copyright © 2017 Arcserve. All rights reserved. Privacy Policy | Support Policy | Terms Of Use

Retention rules define how long records are held in the archive. The DPO can override this for records which meet GDPR criteria.

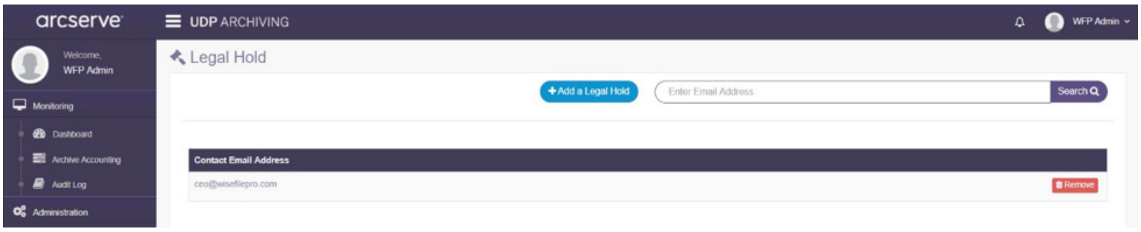
- **Exception(s) –** By identifying exceptions with any of the five policies described in the retention section, the messages are classified and discarded before they reach the archive. To comply with GDPR, a DPO can set an exception on anyone who has made a SAR or may be proactive to remove groups of emails, such as those that go to a specific email address.



From Email Address	To Email Address	Subject	Message Size	Attachment Name	
Julie@epic.com					Remove

Exception rules prevent emails from being archived based on pre-set criteria such as email address, subject, message size or attachment name. Someone with a 'right to be forgotten" request could be set as an exception.

- **Legal Hold –** During a litigation process, legal holds prevent emails from being removed from the archive when their retention policy end date is reached. Message records are held until the hold is released. During a SAR review, the DPO can see messages on Legal Hold and determine the priority. A Legal Hold may be a justification for not removing a record even when a SAR is made.



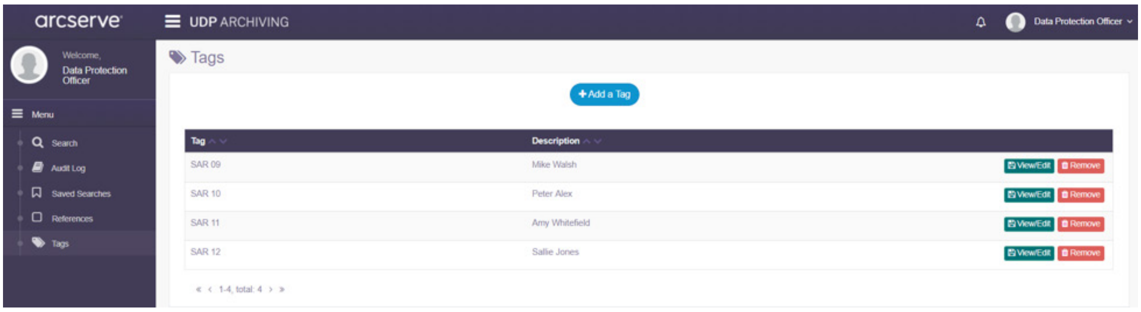
Contact Email Address	
ceo@wisefilepro.com	Remove

Legal holds prevent records from being removed at their end of life. A DPO can evaluate a legal hold on a record found in a SAR search and override the legal hold if appropriate.

Five Steps to Managing Subject Access Requests

A consumer can make a Subject Access Request (SAR) if they believe an organization has their personal, confidential information without a justified reason. UDP Archiving arms the DPO with tools necessary to quickly manage these requests.

Step 1: Create a Tag/Folder for the SAR. The DPO can manage many SAR's at one time.



Tag	Description	
SAR 09	Mike Walsh	View/Edit Remove
SAR 10	Peter Alex	View/Edit Remove
SAR 11	Amy Whitefield	View/Edit Remove
SAR 12	Sallie Jones	View/Edit Remove

« ‹ 1-4, total: 4 › »

A DPO can mange many SAR's at one time and isolate the results into separately managed folders which are referred to as Tags.

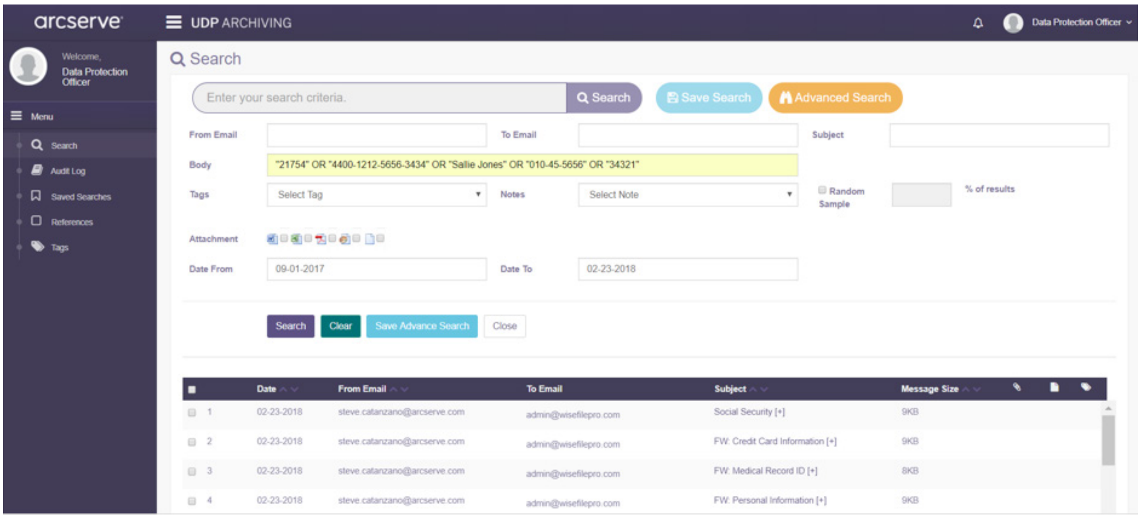
Step 2: Perform a search of the archive and all records based on advanced search criteria.

UDP Archiving has extensive eDiscovery capabilities that can be leveraged by the DPO. For example, a search can be made up of any of the following variables:

- **Email addresses: sent by and sent to addresses**
- **Subject line text**
- **Email body text**
- **Date Ranges**
- **Attachment type (if any)**
- **Advanced functions**
    - Boolean connector allows you to narrow a search using AND, OR, NOT.
    - Fuzzy searching by only entering the first character: john* would also find Johnathan
    - Exact match: "john smith"

All email records are full-text indexed and include any attachments. These search functions allow a DPO to perform a search and locate records for review. A search could be as simple as the name of the individual in the SAR, or more advanced criteria such as a credit card number.

When a search is performed, all of the results will appear for the DPO.



From Email:

To Email:

Subject:

Body: "21754" OR "4400-1212-5656-3434" OR "Sallie Jones" OR "010-45-5656" OR "34321"

Tags: Select Tag

Notes: Select Note

□ Random Sample   % of results

Attachment: ☑ □ □ □ □ □

Date From: 09-01-2017

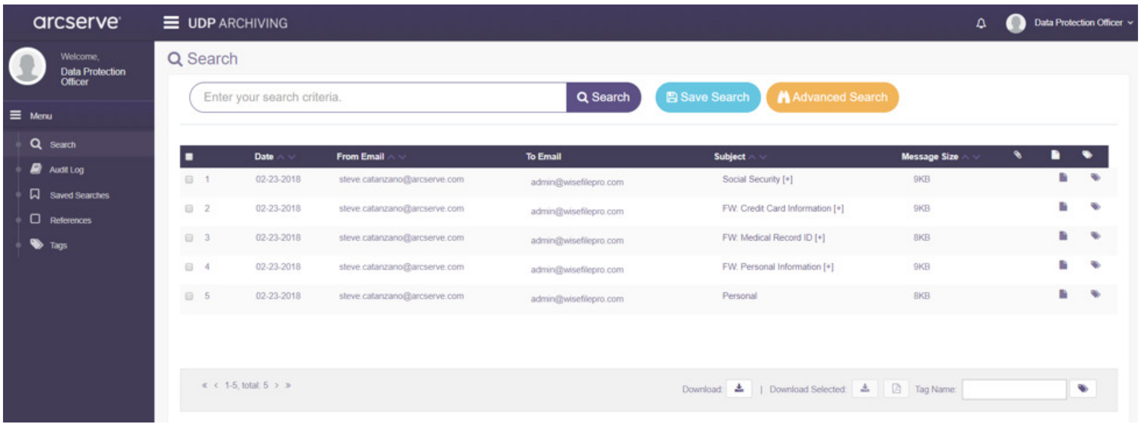
Date To: 02-23-2018

■	Date	From Email	To Email	Subject	Message Size
□ 1	02-23-2018	steve.catanzano@arcserve.com	admin@wisefilepro.com	Social Security [+]	9KB
□ 2	02-23-2018	steve.catanzano@arcserve.com	admin@wisefilepro.com	FW: Credit Card Information [+]	9KB
□ 3	02-23-2018	steve.catanzano@arcserve.com	admin@wisefilepro.com	FW: Medical Record ID [+]	8KB
□ 4	02-23-2018	steve.catanzano@arcserve.com	admin@wisefilepro.com	FW: Personal Information [+]	9KB

In the example above, the search string includes a credit card number, social security number, medical ID, individual's name and a driver's license. The search results will return any email records containing any one of these criteria.

Step 3: Locate Relevant Records

Review and Tag: The DPO has the option of tagging all returned results to “SAR folder 12” (example) or reviewing each message and only tagging relevant records after confirming them. If all are moved to the folder, the DPO can review them at a later time. Any search criteria used will be highlighted when messages are reviewed. For example, if you are looking for a credit card number, it will be highlighted.

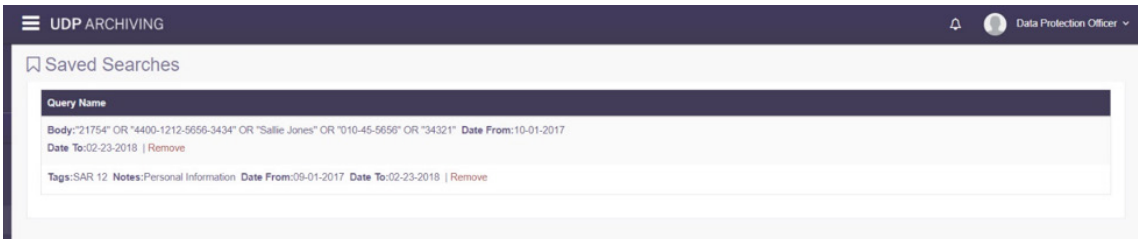


■		Date	From Email	To Email	Subject	Message Size
□	1	02-23-2018	steve.catanzano@arcserve.com	admin@wisefilepro.com	Social Security [+]	9KB
□	2	02-23-2018	steve.catanzano@arcserve.com	admin@wisefilepro.com	FW: Credit Card Information [+]	9KB
□	3	02-23-2018	steve.catanzano@arcserve.com	admin@wisefilepro.com	FW: Medical Record ID [+]	8KB
□	4	02-23-2018	steve.catanzano@arcserve.com	admin@wisefilepro.com	FW: Personal Information [+]	9KB
□	5	02-23-2018	steve.catanzano@arcserve.com	admin@wisefilepro.com	Personal	8KB

The search result above show five records which contain one or more of the personal items searched.

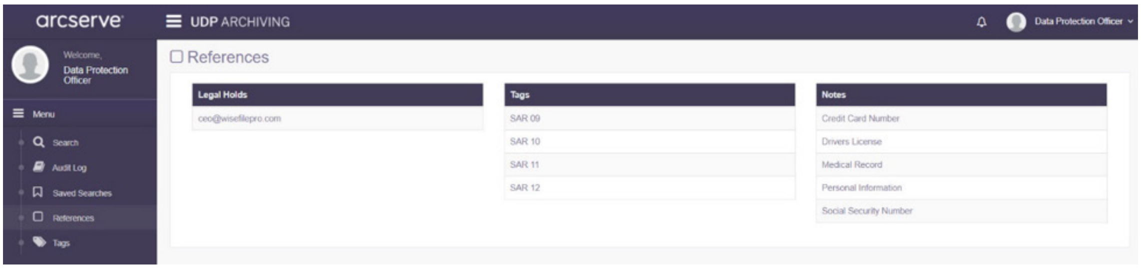
Multiple Searches: For each SAR, the DPO may need to run multiple searches. They can add them into the SAR folder and continue to search, review and tag until all the records are found.

Saved Search: The DPO can save a search for a specific SAR, or save a pre-set search criterion to be performed on any future SAR.



Query Name
Body:"21754" OR "4400-1212-5656-3434" OR "Sallie Jones" OR "010-45-5656" OR "34321" **Date From:**10-01-2017 **Date To:**02-23-2018 | Remove
Tags:SAR 12 **Notes:**Personal Information **Date From:**09-01-2017 **Date To:**02-23-2018 | Remove

The DPO can save a search or set of search criteria to perform again in the future.



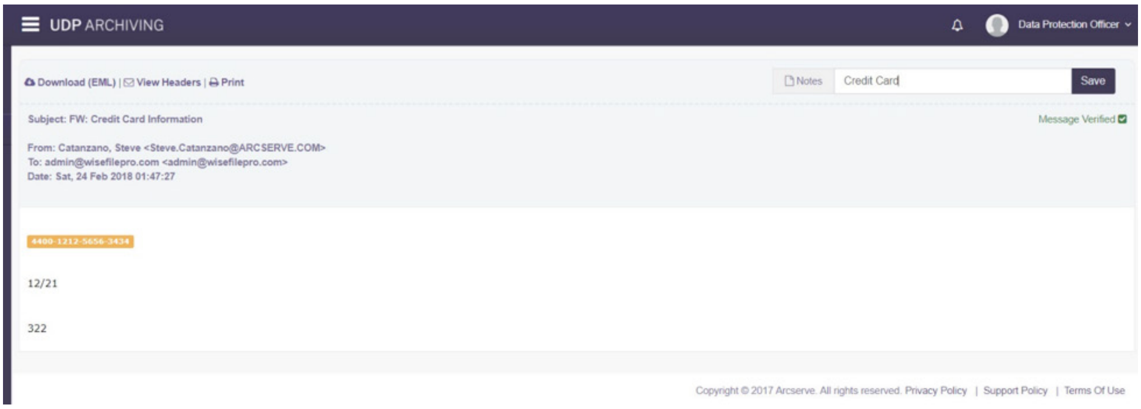
Legal Holds
ceo@wisefilepro.com

Tags
SAR 09
SAR 10
SAR 11
SAR 12

Notes
Credit Card Number
Drivers License
Medical Record
Personal Information
Social Security Number

The references section shows a DPO the tags (folders) they created for each SAR they are working on, any notes they are using, and the status of legal holds.

Notes: On each record, the DPO can add specific notes for future references. A DPO has the right to exclude records if there is a valid reason they exist, and the organization has the right to maintain the records. The DPO can use notes to track the reason a message is being included or excluded.



Notes: Credit Card

Subject: FW: Credit Card Information

From: Catanzano, Steve <Steve.Catanzano@ARCSERVE.COM>
To: admin@wisefilepro.com <admin@wisefilepro.com>
Date: Sat, 24 Feb 2018 01:47:27

4400-1212-5656-3434

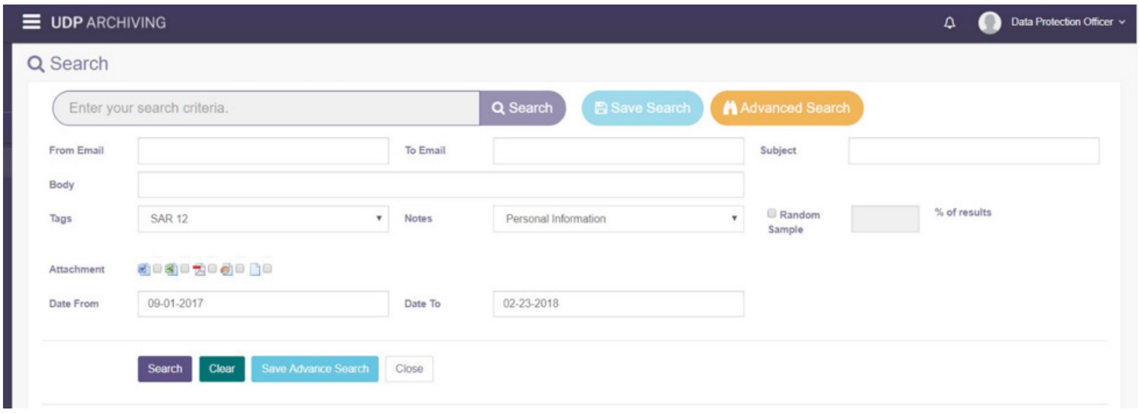
12/21

322

Copyright © 2017 Arcserve. All rights reserved. Privacy Policy | Support Policy | Terms Of Use

When researching email records, the searched criteria is highlighted as seen above. The DPO can also apply notes, such as a reminder of the criteria that was searched. Records can be printed or exported as a message file.

Results: When the DPO has completed this process, a set of relevant records for the SAR have been found, reviewed, and identified in a specific folder. At any time, the DPO can review the folder contents and search within the folder based on date ranges, notes applied, and all other advanced search features if the criteria have changed in any way.



From Email:
To Email:
Subject:
Body:
Tags: SAR 12
Notes: Personal Information
□ Random Sample
% of results
Attachment: ☑ □ □ □ □
Date From: 09-01-2017
Date To: 02-23-2018

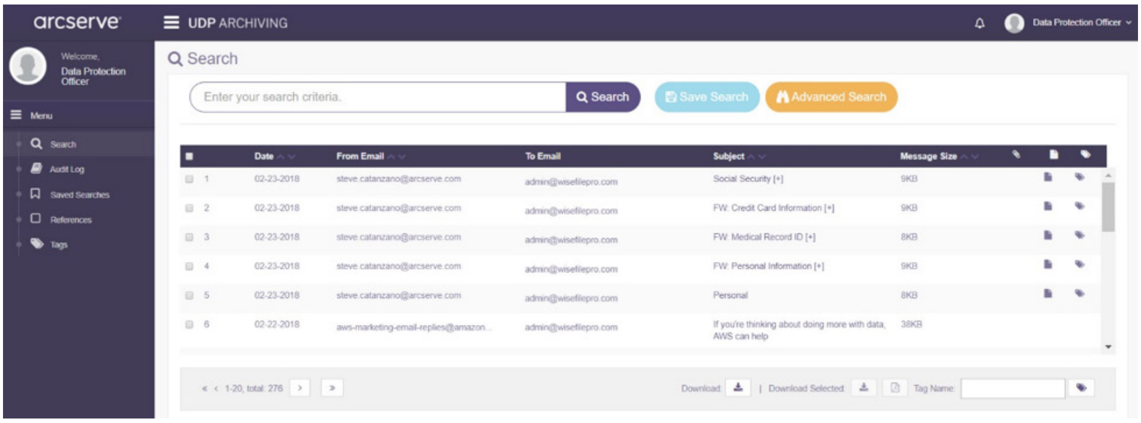
Shown above, the DPO can return to the SAR folder by selecting it from the tag dropdown. A DPO can also select notes which were added to email records, and other search criteria within the SAR folder.

Important: Another benefit of an email archiving system is that it maintains a full set of records and since most data in an organization goes through email at some point in its life, this becomes a great source for a DPO to track down other records and perform additional "detective" work as needed, potentially locating other sources of storage for the data in the organization. For example, if the search finds a record with a spreadsheet attachment that contains the violation, the DPO can use the email record to track down the sender, recipient and file to have it removed from the company. A search on the name of the offending spreadsheet can also be conducted in other systems or storage shares (with other search tools).

Step 4: Produce Records for SAR

Now that all of the records have been located, the DPO can respond to the SAR and identify what email records exist. The DPO can export the records as email files, convert them to PDF files, print them or create a spreadsheet describing each record.

GDPR rules require the DPO to identify the records and inform the SAR what records exist. The SAR can then respond with a request for action to be taken by the DPO such as removing the records.



		Date	From Email	To Email	Subject	Message Size
□	1	02-23-2018	steve.catanzano@arcserve.com	admin@wisefilepro.com	Social Security [+]	9KB
□	2	02-23-2018	steve.catanzano@arcserve.com	admin@wisefilepro.com	FW: Credit Card Information [+]	9KB
□	3	02-23-2018	steve.catanzano@arcserve.com	admin@wisefilepro.com	FW: Medical Record ID [+]	8KB
□	4	02-23-2018	steve.catanzano@arcserve.com	admin@wisefilepro.com	FW: Personal Information [+]	9KB
□	5	02-23-2018	steve.catanzano@arcserve.com	admin@wisefilepro.com	Personal	8KB
□	6	02-22-2018	aws-marketing-email-replies@amazon...	admin@wisefilepro.com	If you're thinking about doing more with data, AWS can help	38KB

« ‹ 1-20, total: 276 › »

Once the DPO has identified any email records for the SAR, they can be exported as email files into a zip file, converted to PDF's or printed from the bottom row of the screen above.

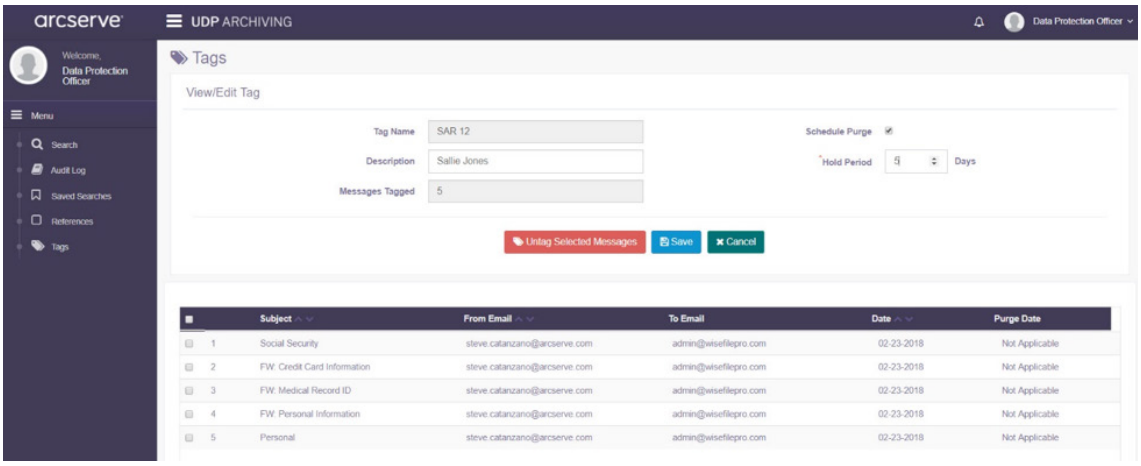
The DPO can also be proactive and remove the email record before responding. See step 5.

Step 5: Perform "Right to be Forgotten"

If the SAR responds requesting action to be taken on the email record, the DPO has the power to remove the records from the archive.

- Return to UDP Archiving
- On the left panel, go to manage tags
- Find the SAR tag for this request and pull up the results
- Change the date to the day you want these messages removed
- On that day the messages will be purged from the system

Once completed the DPO can report to the SAR that the records have been removed.



Tags

View/Edit Tag

Tag Name SAR 12

Description Sallie Jones

Messages Tagged 5

Schedule Purge ☑

*Hold Period 5 Days

□		Subject	From Email	To Email	Date	Purge Date
□	1	Social Security	steve.catanzano@arcserve.com	admin@wisefilepro.com	02-23-2018	Not Applicable
□	2	FW: Credit Card Information	steve.catanzano@arcserve.com	admin@wisefilepro.com	02-23-2018	Not Applicable
□	3	FW: Medical Record ID	steve.catanzano@arcserve.com	admin@wisefilepro.com	02-23-2018	Not Applicable
□	4	FW: Personal Information	steve.catanzano@arcserve.com	admin@wisefilepro.com	02-23-2018	Not Applicable
□	5	Personal	steve.catanzano@arcserve.com	admin@wisefilepro.com	02-23-2018	Not Applicable

If a request to be forgotten is then received, or if the DPO deems the records unnecessary and wants to proactively remove them, the Tags screen above shows that the DPO can set a new Hold Period for the records (shown as five days). This will override the records normal retention time. Once the time has passed the DPO can respond that the records are removed. Prior to this, the DPO can use these records to trace back into the organization and find the originators and original records.

Periodic Review: We recommend saving the search criteria for the SAR and running the search again in the near future as well as more global searches for PII. This will identify if new records have been produced somewhere in the organization. By following the email trail, you can quickly determine where the records are being produced and prevent them in the future. If this is happening for one person, it may also be happening for many more.

UDP Archiving gives you the intelligence you need to find the root of the problem.

Data Protection

A key part of GDPR is protecting stored data. Organizations with UDP Archiving leverage five key safety measures to ensure compliance:

- ***Encryption:*** Every stored message is encrypted, which prevents unauthorized access and message tampering.
- ***Unalterable Records:*** All email records are stored in an unaltered state – they remain in their original format, unchanged in any way.
- ***Access Control:*** A tiered level of controls provide access to email records by authorized users, including the use of Captchas on login to insure the user is a person and not a system attack.
- ***HTTPS/SSL Certificate:*** For web access, the site is secured with an SSL certificate which can also be restricted to known IP addresses and set up behind a corporate firewall.
- ***Transport Layer Security (TLS):*** TLS can be enabled to provide an encrypted connection between the mail server and archive for transport layer protection.

Minimizing Data and Monitoring for GDPR

Two important requirements of complying with GDPR are minimizing files which contain personal information and monitoring for stored information. UDP Archiving addresses these requirements with the following:

Single Instance Storage – SIS is used to reduce the amount of storage used by retaining messages one time. For example, if an email is sent to one hundred employees, that record is only stored once in the archive.

Exception Rules – These allow the company to prevent messages from being archived based on pre-set rules, such as email to or from a specific IP address, messages with an identifiable subject, size, or a named attachment.

Proactive Reviews – A DPO can set up a defined search criteria and review all received messages. This makes it easy to routinely check to see if emails are being sent which violate company GDPR and other regulatory policies.

Locating Sources – Archiving acts as a central repository of email records, and because most of an organizations content and communications are captured in email, it becomes a way to identify issues and trace them back to the originator. For example, if an email is identified as having a list of customer credit card numbers, the DPO can immediately know who sent the information by the email trail, and subsequently remove it from the archive and its source. It also serves to determine if it is an on-going violation.

Putting together your GDPR toolkit

Organizations need to implement tools and processes now to comply with GDPR and other regulatory policies. By leveraging powerful email archiving technology, your business can greatly reduce its compliance risk – and subsequent hefty fines – while improving the efficiency of compliance processes. Contact Arcserve for a free GDPR email archiving assessment.

For more information on Arcserve, **please visit** arcserve.com