Winckworth Sherwood

Winckworth Sherwood deployed two enterprise solutions to bring data workflows in line with GDPR requirements. In doing so, the firm strengthened data protection and enabled searchability of image files within its document management system.

How UK Top 100 Firm Winckworth Sherwood strengthened data protection for GDPR compliance

The business need - improve data protection and search capabilities

Keep sensitive documents and client information protected as required by the GDPR

Manage the most common risk of data leaks – missent emails

Find an alternative to 'delay on send' to prevent human error in email

Respond with confidence to Data Subject Access Requests under the GDPR

Convert non-searchable image-based files to text-searchable PDFs

Eliminate the need to OCR at the point of scanning on Multi-Function Devices (MFDs)

Find an OCR framework that would integrate with existing systems, including NetDocuments

About Winckworth Sherwood
A member of the Legal 500 UK and relied on by some of the UK's largest organisations, Winckworth Sherwood (WS) is a full-service law firm with a diverse client base. Since as far back as 1777 the firm has established its reputation for delivering high levels of client service in high value, high profile projects.

Finding an all-in-one solution to manage metadata and stop missent emails
Every file contains metadata, and metadata like author properties and embedded objects have the potential to include personally identifiable information. Global regulations like the GDPR require businesses to keep personal information safe from leaks. Winckworth Sherwood needed to raise awareness about data leak risks and provide appropriate tools to mitigate this. Without accounting for metadata security, sensitive document data can easily be leaked. Information such as Track Changes (e.g., deleted text you thought was gone), hidden text, or comments on documents not intended to be shared can be inadvertently sent.

The other part of the firm's data protection strategy was managing the risk of missent emails. Christel Aguila, Head of IT at Winckworth Sherwood could see how, without the right tools in place, "it was one of the most dangerous, if not the most common cause of data leaks," and could end up costing the firm thousands of pounds in fines. Christel recognised that "addressing an email to the wrong person or attaching the wrong file are easy mistakes to make." The IT service desk has in the past received frantic calls asking if a missent email can be recalled. Unfortunately, once an email has been sent, it's nearly impossible to undo the damage. Addressing the issue by putting a delay on sending an email isn't effective. "Even if you remember you made a mistake, it might be too late and there's nothing you or IT staff can do," she said.

To this end, Winckworth Sherwood trialled cleanDocs since it is the only product to offer two points of defense against missent emails: metadata cleaning and email recipient checking.

With cleanDocs, email users can check the recipient list for external or blacklisted email domains and confirm that they are all as intended. Within the same prompt, users can action metadata cleaning to remove hidden information. This ensures that only the right information is sent.

"Because cleanDocs is configurable and so simple to use, the extra checks work really well. It's effective at stopping you in your tracks before you send an email out incorrectly – particularly on a manic day," said Christel.

Since deploying cleanDocs, Christel says there have hardly been any missent email reports being raised with the service desk, and if there was, it was from one who has not enabled it on their PC and has since requested for it to be activated. Even the IT department now uses the feature to prevent missent emails. "We don't want quotes or contracts to go to the wrong supplier, for example."

Back-end OCR processing to make all files text-searchable for data discovery

100% searchability is critical for Data Subject Access Requests (DSARs) under the GDPR. Law firms are aware this can become a challenging task, and for WS, there were gaps that needed filling. "There were thousands of dark data images and documents in our DMS," said Christel. "If you're not able to fully search the documents' content, then that is a concern and a business risk."

To minimise the impact of converting dark data to text-searchable PDFs on staff productivity, Christel looked for an OCR search, assess, and convert solution that could be switched on and run without any staff intervention. This led WS to contentCrawler, which runs fully automated in the back-end of systems, crawling for files that require OCR processing. "It just made perfect sense to have something working for us in the background without users or IT having to worry about it."

Deploying contentCrawler's OCR framework in the back-end – in this case within NetDocuments, meant that any newly profiled files, plus legacy files already saved, could automatically be made searchable. "When we moved to NetDocuments, it was a no-brainer to have contentCrawler. We integrated it prior to going live which meant that as non-searchable files were being migrated, they were automatically tagged and OCR'd. By the time we went live, we had most of the previously invisible documents searchable. It continually does its work in the background, so it's a powerful tool to have."

contentCrawler has saved time and effort when it comes to OCR as a workflow. "We eliminated the need to OCR documents when you scan from Multi-Function Devices (MFDs) because anything that hits NetDocuments will be converted into a searchable document."

contentCrawler has also saved the IT department time since they don't have to OCR documents, implement OCR functionality on MFDs, or train people. "contentCrawler just sits in the background and does the job of OCR'ing for us whatever the source - i.e., scanned from a device, downloaded from an external portal or sent as an attachment by email."

"The best thing about both cleanDocs and contentCrawler is they help facilitate GDPR compliance without undermining productivity," said Christel.