

TAKE YOUR DATA WITH YOU

NATASHA RAWLEY, THE FILE QUEEN

Hello there, LPM readers – can you believe we’re nearly already through the first quarter of 2017? Businesses now have just over a year to get ready for the EU’s General Data Protection Regulation – so let’s press on with step four of the Information Commissioner’s Office’s 12 steps to the GDPR: individuals’ rights.

You may remember that last month we covered subject access and the right to be forgotten (if you missed last month’s column, download the February issue at www.lsn.co.uk/lpmmag).

Let’s dive into: preventing direct marketing. Whether your marketing department is internal or external, it’s your responsibility to make sure you have permission to contact people – your contacts must opt in to be contacted by mail, email or telephone. This includes existing contacts – even those who have previously agreed to let you contact them will need to re-agree in line with the GDPR changes.

At File Queen HQ we’re currently emailing all individuals on our database (both current and potential clients) and asking them how they prefer to be contacted, and if they want newsletters and special promotions. It’s a lot of hard work, so I suggest you start doing this now.

Next, you need to prevent automated decision-making and profiling. The ICO explains: “When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that restriction is respected in the future.” If a client approaches your firm for legal services, they share information with you – but do you then share that data with insurance companies or mortgage brokers? On completion, do you then send client data to partner firms that might market the client? This is processing data and sharing data with a third party – and you need to know: do you have permission to do this? Furthermore, do you know that these third parties will also process data with strict GDPR procedures?

Another important issue with individuals’ rights is data portability: individuals’ rights to obtain and reuse personal data for their own purpose, and to easily move, copy or transfer it from one IT environment to another in a safe and secure way, without hindrance to usability.

Several firms we work with already have great procedures for dealing with file handovers. First, they validate the claim for information by ID checking (matching to previously scanned copies of their ID), and then send notification of an on-demand scan to us. The relevant files are then scanned with optical character recognition, put into pdf format, placed onto an encrypted portable hard drive and delivered to the business.

Once the practice has added any additional electronic documents, we then relock the hard drive and deliver it to the person who’s asked for their data and help to provide a full audit trail.

The main focus on this step is all about process and accountability. It may seem like overkill, but it’s there to protect us. If you need help, go to a GDPR and data protection office course – I’ve been on a few and they are so valuable. And we are here to help, so contact us. [LPM](#)



“Whether your marketing department is internal or external, it’s your responsibility to make sure you have permission to contact people.”

ABOUT

ADDS
Saving firms from paper hell
Contact Natasha on:
0800 328 0272
www.archivestorage.net
[@Thefilequeen](#)

