SPONSORED EDITORIAL

QUESTION TIME FOR COMPLIANCE

NATASHA RAWLEY, THE FILE QUEEN

So, here we are in the week of the GDPR activation and wow – it has been so busy at File Queen HQ at ADDS. By the time this column goes out, we will have helped over 600 clients adapt record management processes to bring them more in line with the GDPR regulation, and we need a desert Island break!

I know we're all sick and tired of speaking about GDPR, but I wanted to take this opportunity to share with you some of the internal process we have in place at ADDS that have been part of our day-to-day processes for many years. They are not totally related to record management but I think may bring a little bit of extra help to you as a GDPR checklist for your internal operations on a security and data breach prevention level.

Do all of your team members, suppliers and clients sign in and out of site? Are supplier and clients' issues with security processed on checkin? If there was a data breach, would you be able to pull a list of all people onsite at that time and date? Are team members across all departments and levels security checked? Are suppliers escorted onsite at all times? Or are they allowed to just wander the site? Random suppliers onsite who have not been security checked by you are always a security risk and should be escorted at all times.

Do you ask clients for photo ID upon entry to the building. Are they who they say they are? Do you have a security office closure checklist for your practice? Is there a process for the last person who leaves the building or department, which can be ticked off and documented as complete? Are those windows closed? Are the desks clear? Are all computers switched off? Are the file storage areas and cabinets locked? Are fire exits checked? If you have a cleaning company servicing your office out of hours, what security checks do does it run on team members? Do you have a clear-desk policy for your practice, or do the cleaners have access to confidential information when you are not there?

Do you regularly check your team's PCs and laptops for locally stored documents? Best practice is that documents are not locally stored; not only for back up but also in case of a data breach. What if that laptop was left on the train or the PC stolen? Does it have client information stored locally on it? How will you know what information it is in order to alert the client to a data breach? Do your team members regularly empty their laptop/PC recycling bins? Best practice would be to do this twice a day. Again, if this computer was in the wrong hands, what documents would be in those recycle bins that could be easily recovered?

How often does your system request a password change? The minimum should be every 30 days, with strong password requirements such as upper and lower case, symbols and numbers required.

Are team members in the practice of regularly locking their PCs and laptops when they leave them? Even for a tea break? If not, this is a potential data breach. We all like some internet freedom but the hazards that social media sites and personal email logins like gmail can pose to an IT network can be devastating. Best practice would be to deactivate any access to these sites.

Are your team constantly reminded to run daily security scans on their PCs and laptops? Do they sign a document to say they have completed this daily? Every day? Do you control portable media devices on PCs and laptops, or can team members plug in USB sticks and run mass data downloads or upload without IT consent?

Personal mobile phones – are team members allowed to use personal mobile phones for emails or at their desk? What if a personal mobile phone went missing – what information would be on it that causes a databreach for you? Could a member of your team be taking photos of client information with their personal mobile phone?

All sounds very paranoid, doesn't it! But with the constant danger of a data breach, why shouldn't practices be paranoid? If you want to download the checklist tool we use internally for our team members, you can find it here: www.archivestorage.net/news/gdpr/. LPM

ABOUT

ADDS
Saving firms from
paper hell
Contact Natasha on:
0800 328 0272
www.archivestorage.net
@filequeenadds

Would you like your practice to be paper lite?

1. Call ADDS, we can help!

2. Book your free consultation.

3. We organise and pack.

4. Then uplift and transport to our secure records management facilities.

5. Each file is barcoded and indexed.

6. Then stored safely and securely.

7. You can easily request a hardcopy or electronic return via our system.

Archive Document Data Storage

You can count on us

Contact us now for a free consultation

☎ 0800 328 0272 | www.archivestorage.net | filequeen@archivestorage.net

@filequeenadds | @filequeenadds | ArchiveDocumentDataStorage