A Practical Guide for Managing Data Risk with consideration for GDPR

March 2018

1. Have a Data Retention & Destruction Policy

Many firms will already have a document retention policy, but the chances are that, if it has not been updated for some time, it may not be quite as broad as it needs to be. The Law Society of Scotland has for some years now, provided guidance on the ownership and destruction of files.

The data protection regime goes somewhat further now, and firms should be considering a policy that addresses data storage/retention in the round, including:

- Physical files
- Electronic documents
- Emails
- Client data held on CRM systems or third party systems
- Staff data held
- Data stored on portable devices, and office equipment, including telephone call recordings, and data stored on copiers and printers (you should be aware that most printers and copiers will store a considerable volume of data unless wiped before selling or otherwise replacing)
- Data held in cloud systems and IT back-ups.

2. Address your hard copy document risks

Paper is not necessarily either more or less secure than electronic data, but it must not be forgotten when considering implementing changes in readiness for GDPR. Your paper-based data is also subject to many of the new regulations. It also has its own particular risk issues. Some of the Risks include:

Unauthorised copying of hard copy documents

These days, with the advent of quality cameras in smart phones, and email enabled scanners, taking a sneaky copy of a document is a far less risky form of information theft.

Taking documents out of the office

There is no doubt that, for many of us, reading a hard copy document while travelling remains easier and more reliable than trying to access documents online. While portable devices, if properly set up, are encrypted and can be remotely wiped, the same cannot be said for paper files left on a train.

Loss of documents

Documents still get lost between the office and archives, and, in case of fire and flood, can be destroyed entirely.

Risk Mitigation Suggestions for your consideration

- Undertake an audit of your paper documentation (at least insofar as it contains personal information), rationalising copies insofar as possible. While electronic storage is not a panacea, scanning and shredding documents and correspondence as they come in will reduce the risk of some forms of theft.
- Minimise the number of hard copy documents you store. As well as reducing the risk of inadvertent data breach, this also makes it much easier accurately to track compliance with data protection requirements.
- Implement a policy that forbids the removal of original documents, and only permits copies subject to a 'destruction after use' rule. This will also help prevent the existence of multiple copies of a document.
- Send completed matters to secure archive at the earliest opportunity following a proper post completion file review, keeping a record of the archived material, and types of personal data contained therein. We suggest using electronic archiving where possible for the bulk of a file.

3. Review your document retention rules

There are no hard and fast rules for client document retention, and GDPR does not alter the current framework in that regard. However, the preparation for GDPR does provide a good opportunity to review your current arrangements. Where many firms could benefit is from a re-evaluation of their procedures for identifying and managing documents/data that should now be destroyed or deleted.

GDPR requirements regarding the storage of personal data

"Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Personal data may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, or scientific, historical, or statistical purposes in accordance with Art.89(1) and subject to the implementation of appropriate safeguards." ***(Article 5, GDPR)***

This needs to be balanced against your legal and regulatory retention requirements and the need to retain information for long enough to provide material for an adequate defence in the event of a claim. Firms should always consider their own individual specific circumstances when determining timescales for destruction. While the GDPR does forefront the rights of data-subjects, as long as you can properly explain why you process the data and have set a fair retention period, the firm's legitimate interests should be respected, assuming of course that you have implemented sufficient measures to protect the data.

Firms must also take into account the retention/ destruction requirements relating to Client Due Diligence, as detailed in the 2017 Money Laundering regulations.

Whatever your policy determines, you should ensure that your letter of engagement explains clearly

- who 'owns' the client file, and what that means
- how long you will retain the file for, how it will be stored, and what will happen to the file after that time
- any costs which may be payable relating to storage, retrieval and copies of [parts of] the file.

4. Establish & Maintain an effective procedure for identification and deletion of relevant records

Having a meaningful policy on data retention and destruction is one thing. Ensuring that it is implemented in practice is quite another.

Employing someone to go through file records and notifying fee earners when a data-retention period has expired is costly, time consuming, and also does not guarantee that the information is acted upon by a busy fee earner. An alternative approach, that electronic documents are automatically permanently deleted after the retention period has expired, is also problematic.

As detailed above, complying with data destruction policies where hard copy documentation is concerned is more difficult again – thus the incentive for many firms to move to online storage insofar as possible.

Further Risk Mitigation suggestions for your consideration

- If you do not already have an 'Information Asset Register' in place, now is the time to scope and implement one in readiness for the May 25th deadline. At its simplest, this can be a centrally stored spreadsheet (in respect of client data held, you will want a separate spreadsheet that relates to staff and other management data held) which is completed as a matter of course at the conclusion of any matter. Fields should include: nature of the data (including the categories of personal data), purpose of the processing, a description of the categories of data subjects data format, categories of recipients to whom the data will be disclosed (including any transfers outside the EEA), the location of the data, and the relevant timescales for destruction of the data. The register should also include the contact details of the controller or processor and, where appointed, the Data Protection Officer. There should also be a general description of the technical and organisational measures employed to keep the data security. The data should be reviewed regularly as part of any file audit process.
- Ensure that marketing preferences are adequately captured– and that marketing campaigns are run from a current version of the list , rather than relying on a past mailing/distribution list.
- Review email storage at regular intervals, and speak to your IT department about arranging a central email deletion policy, automatically deleting emails from the server after a set period.
- Review your data storage systems, including document management, email and other records management systems. Using integrated systems from reputable suppliers should help ease the administrative burden of GDPR compliance.

Please note that the purpose of this article is to provide a summary of and our thoughts on aspects of the General Data Protection Regulation.