

# Broken R

**Records management is not an area the legal profession can afford to be lax about: it's now against the law to hoard files indefinitely. Martin Bradley opens the archive door**



## MAIN POINTS

- **Records management**
- **Data Protection (Amendment) Act 2003**
- **Implications for law firms**

**R**ecords management in Ireland has traditionally been a matter of filing everything, regardless of currency, just in case it might be needed for some future, unspecified, purpose. However, with the advent of the *Data Protection (Amendment) Act 2003*, this long-established culture of hoarding has reached a legal end – not only are organisations breaking the law by keeping everything indefinitely, but individuals are personally liable for penalties up

to €100,000 under section 25 of the act.

Though applicable to all sectors of Irish business, the legislation is particularly relevant to the legal profession. For example, conjure up an image of an old-style solicitor's office and you'll surely think of parchment and tomes gathering dust. Thankfully, those days are a thing of the past, but records management is not an area the legal profession can afford to be lax about. The confidentiality of the information retained and the volume of files

# RECORDS

generated are key issues, but now with this legislation comes the additional pressure of being the last profession that should be found to be in breach of Irish law.

As Tom Maguire, Deputy Data Protection Commissioner, recently said: “As long as you have a records management policy, you won’t get into trouble with us; if you don’t have one, then this is an issue of concern.”

## Key aspects of the act

There were a number of key changes under the 2003 extension to data protection legislation. Firstly, it was extended to apply to manual records held in an organised filing system (and before you ask, pleading that your files are disorganised can’t be used as a defence – if it’s on a file, then it’s part of a filing system).

Secondly, the extension states that appropriate security measures must be taken against unauthorised access, unauthorised alteration, disclosure or destruction of data – again this relates to manually kept records. Thirdly, and arguably most importantly, it states that *data shall not be kept for longer than is necessary* for the original purpose it was collected.

In relation to the third point, the Office of the Data Protection Commissioner’s website ([www.dataprotection.ie](http://www.dataprotection.ie)) offers some practical advice: “You should pay particular attention to old information about former customers or clients, which might have been necessary to hold in the past for a particular purpose, but which you do not need to hold any longer. If you would like to retain information about customers to help you provide a better service to them in the future, you must obtain the customers’ consent in advance. The same applies to paper records. Good housekeeping would also dictate that you regularly review the need to retain records.”

This clearly has serious implications for many law firms. The commissioner further asks three simple questions:

- Is there a defined policy on retention periods for all items of personal data kept?
- Are there clerical and computer procedures in place to implement such a policy?
- Is information about old clients routinely purged from your systems?

In practical terms, what this means is that every organisation needs to have a records management policy. It is no longer acceptable to have a

basement containing files on all your clients, past and present, to have *ad hoc* arrangements for retrieving and tracking files, or to keep everything indefinitely.

## Where’s that paperless office?

Fortunately, good records management brings with it a number of benefits beyond legislative compliance. It certainly shouldn’t be viewed as a burdensome exercise that has to be implemented solely for that purpose. A recent study by the University of California at Berkeley came up with some very interesting statistics:

- Offices worldwide used 43% more paper in 2002 than they did in 1999;
- The average organisation makes 19 copies of each document, loses one out of every 20 documents, and office workers can each spend 400 hours a year looking for lost files;
- Between 1% and 5% of all documents are misfiled;
- When email is introduced into an office, the percentage of printed documents increases by 40%.

The 1980s promise of a paperless office has never come to fruition. In fact, and as these statistics show, paper-record generation increases hand-in-hand with technological advancement. This would not be such a problem if record management skills were developing at a similar pace. The confident predictions of the technology industry that paper was a thing of the past, combined with an array of software products sold on the understanding that they did the filing for you, meant office administrators were lulled into a false sense of security. That is, of course, until the problems started.

High-profile instances of government departments being unable to lay their hands on files have led to costly reactive measures, including hiring teams of unfortunates to back-catalogue warehouses full of files that, with proper file maintenance, should have been easily accessible. Recently, the departments of education and health have invested well in cataloguing work, both current and historical, on foot of enquiries, but also to enable that efficient processes are in place to enable the straightforward retrieval of files in the future.

Of course, when we talk about today’s record management, we are discussing a vastly altered landscape. There are classes of records that are nowadays created and stored in exclusively electronic

## SIX ELEMENTS OF A RECORDS MANAGEMENT POLICY

An effective policy:

- 1) Assigns responsibility to staff to ensure that records are properly kept;
- 2) Applies to all paper records, electronic and manual;
- 3) Follows a record's life-cycle from creation to ultimate archiving or destruction;
- 4) Sets out retention periods dictating the length of time that a record is kept in the office, how long it is maintained as a non-current record in offsite storage, and then whether it is destroyed or maintained permanently after a set period of time;
- 5) Ensures security and business continuity. Security is a key element of the *Data Protection (Amendment) Act 2003* and it is important to ensure that information in both electronic and manual filing systems is only seen by those who have a need to see it, and, perhaps more importantly, that it cannot be modified without an audit trail;
- 6) Enables legal destruction of listed records. Quite simply, it is not safe to shred anything unless you have a stated policy that classifies records and allows for their destruction after a certain amount of years in line with legal and administrative requirements.

media. A major sticking point is that employees view these forms of communication, particularly email, as personal correspondence, when in fact they are business transactions that can be easily traced to the issuing organisation. For this reason, law firms and their clients need to be very aware that emails, SMS and 'Messenger' have all been the subject of legal discovery.

### Loose lips

Take, for example, the recent legal wrangle between Microsoft and Netscape. Microsoft learnt the pain of

saving too much archived mail when discovery uncovered a delicate internal mail from AOL, reportedly recounting a meeting with Microsoft boss Bill Gates, which described him as saying, "How much do we need to pay you to screw Netscape?" This led to ancient emails being uncovered and quoted in court. So what should you do? The standard legal suggestion, which Microsoft, Netscape and others have adopted, is to delete all mail, other than those that they are legally bound to preserve.

There must also be a clear policy in place to ensure that no libellous or sensitive business information about your company or its clients is unwittingly passed on.

The most valuable way of increasing efficiency, saving storage space and ensuring legal compliance is to recognise the difference between a record and a document. ISO 15489, the international records management standard, defines a record as "information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business".

The trick to successfully organising your records, both electronic and manual, is being able to identify these key pieces of information and ensure they are properly looked after, while extraneous material (normally around 40% of what is kept by an average business) is disposed of. Once this concept is clearly understood, the next step is producing a records management policy.

To recap on the deputy data commissioner's words, you won't get in trouble if you have a records management policy, but there is an issue if you don't. When beginning this process, it is important to remember that about three weeks' work can bring you very close to implementing an effective records management policy. From cost and time savings to clearing up valuable office space, the benefits of having a clear document retention and destruction policy clearly outweigh the initial work that needs to be done. Every legal firm should make it a priority to implement a solid records management policy and relegate images of dusty old solicitors' offices strictly to the past. **G**

---

*Martin Bradley is a professional archivist and the executive director of Archives Consulting Services Ltd.*

## PUTTING A POLICY IN PLACE

- 1) Survey and list all your files, electronic and manual. Until you know what you have, it is impossible to make any decisions about what to keep.
- 2) Create a file taxonomy. This is essentially a family tree of your records, normally broken down by department or business function, to enable you to group your records together.
- 3) Decide on retention periods. Once you have a taxonomy in place, it is possible to assign retention periods to the various series of files your business creates to ensure that they are only held for the correct length of time according to legal and administrative requirements.
- 4) Index and reference records. It is essential that you are able to find your records when you need to, so many businesses take the opportunity of retroactively assigning reference numbers to all their files and linking these to a database in order to find files. This is also the time to put systems in place that ensure when a new record is created, it is automatically assigned a reference number to track it throughout its life cycle.
- 5) Seek ISO 15489 certification, the international records management standard, and certification that ensures your records management meets that standard. This is useful, both from the point of view of internal audit and in assuring your customers, and the regulatory authorities, that you take records management seriously and have attained a high standard.