

DATA DAY APPROACH TO RECORD KEEPING

The introduction of the 1998 Data Protection Act has had a profound effect on what type of information companies need to retain, as well as which records they should discard and how best to discard them.

According to Gill Watkins, an associate practice support lawyer at law firm Eversheds, organisations need to assess what information they hold, why they need it, how it should be stored and when they need to dispose of it. "Retaining information for too long can be as serious a breach of the Data Protection Act as disposing of it too quickly."

It is vital that organisations set up a retention and disposal policy, says Watkins. The first step is to nominate an individual or a department to take the lead in managing and reviewing any retention and disposal policy. After that, it is important to ensure that the overall aims of the policy are communicated to all staff.

According to the Institute of Chartered Secretaries and Administrators' (ICSA) *A Guide to Document Retention*, by Andrew Hamer, the aims of a retention policy are:

- To ensure that records required to be kept for legal reasons are kept for the appropriate period and in an appropriate manner.
- After a careful assessment of the risks, organisations should minimise the retention of other records while ensuring that the information needs of the business are met.
- To retain records in a manner appropriate to their purpose throughout their life and specifically ensure that records which may

be used in legal or regulatory proceedings are stored in a manner which makes them admissible as evidence.

- Dispose of records that are no longer needed in an efficient, orderly and appropriate manner.
- Ensure that all disposal actions are properly recorded.

Retention and disposal schedules and procedures should:

- Identify which documents and records should be retained and the minimum retention periods for each.
- Identify procedures for selecting records for retention or disposal and the frequency with which that process should take place.
- Specify procedures or the disposal of records (and identify records where special disposal procedures should be followed).
- Allocate clear responsibility for the implementation.

While a document retention policy has been a necessity for decades (storing company accounts and tax records, for example), the Data Protection Act has specific guidelines on how the information should be stored and accessed. More importantly, the Act allows data subjects access to the information held. The Act says that data is information recorded "as part of a relevant filing system". For this purpose, a "relevant filing system" includes a set of information relating to individuals which is "structured either by reference to individuals or to criteria relating to individuals in such a way that particular information relating to a particular individual is readily accessible".

Watkins says it is difficult to cite reliable examples of information unlikely to be covered by the Act.

However, one such example might include a pile of papers not stored in any organised way. Although these might identify individuals, if the information is not "readily accessible" – in the sense that the papers would need to be sorted through before any meaningful information could be extracted – these might be excluded. Similarly, any details which are anonymised, and from which an individual cannot be identified, would also fall within this category.

Timeframes

An issue inextricably linked to what goes onto a personal file is how long information should be held on that file. Although the data code places great emphasis on proportionality and security, it does not seek to answer this age-old question. The only guidance provided is that personal information must not be kept "for longer than is necessary" but equally should not be deleted "where there is a real business need to retain it". This is another area where adopting a policy approach has real advantage. Organisations need to bear in mind any professional guidelines or relevant legal time limits on claims. There is no practical substitute for evaluating the need for, and relevance of, a particular document in each instance. There may be longer retention periods for some documents than others, or different needs for some employees. Possible examples include:

- Application forms – for the duration of employment
- References – one year
- Payroll and tax information – six years
- Sick leave records – three years
- Annual leave records – two years
- Unpaid leave/special leave records – three years
- Annual appraisal/assessment records – five years

- Records relating to promotion, transfer, training and disciplinary matters – one year from end of employment
- References given/information to enable reference to be provided – five years from the reference or end of employment
- Summary of record of service – 10 years from end of employment
- Awards relating to accident or injury at work – 12 years

While organisations need to be aware of the timeframes needed to store documents and when they need to be destroyed, they also need to be aware of the wider implications of the term 'document'. For example, under the Criminal Justice Act 1988, which sets out rules for the admissibility of documents as evidence in criminal trials, a document is defined as "anything in which information of any description is recorded". For the purposes of the Act, a document could include any type of information stored in any form, on any media. It could be information in the form of words, numbers, pictures, maps, plans, sounds, musical notes and so on. The information could be printed, embossed, recorded, processed, engraved or digital, and could be held on paper, microfiche or computer hard-drive.

Neil Hodge

A wide range of Briefings can be found at www.financialdirector.co.uk/briefing

Useful links

- *The ICSA Guide to Document Retention* is at www.icsapublishing.co.uk
- *The Data Protection Act* can be found at www.dataprotection.gov.uk
- Email Gill Watkins at gillianwatkins@eversheds.com