

# How long should I keep data for?

*Stephanie Pritchett, Principal at Pritchetts, discusses the requirements for retaining and destroying data*

It is tempting to answer the question of how long should data be kept for with the unimaginative, 'how long is a piece of string?' Recent case law has established that if you hold the string and are in control of it, then it is you who are in the best position to say how long it is. This article explains more about this knotty issue.

With ever advancing technology, it is becoming increasingly cheap and easy to store information, either on your own servers or in the cloud. In the past, IT and IS Managers may have constantly asked workers to delete data in order to stop servers from crashing but this has tended to become less problematic in recent years. With this ease of storage, however, comes a lethargy or reluctance to delete information electronically that 'may be needed some day'.

Yet at the same time, we are reminded by the Information Commissioner's Office ('the ICO') that it is not acceptable to store information 'indefinitely, just in case'. To do so would, in most cases, be in breach of the Data Protection Act 1998 ('the DPA').

There are, therefore, risks of data protection breach involved in storing information too long. On a practical level, there are also reasonably high costs of storing information online as well as the warehousing of paper records.

On the flip-side, there are risks involved where information is deleted too soon, for instance where this is done before the end of that data's useful life. Indeed, the ICO has stated that it understands that "discarding data too soon would be likely to disadvantage your business and, quite possibly, to inconvenience the people the information is about as well".

It is useful, therefore, to go back to basics and look at the rules under the DPA relating to the storage of information, why you should consider creating a Data Retention Policy and what information that policy should contain. The information may also be helpful when reviewing policies.

## What does the DPA say about retention of data?

The Fifth Principle of the DPA states: "Personal data processed for any

purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes."

This means that personal data should only be retained for a limited time, linked to the original purpose for which the data were obtained. While this may seem like a straightforward requirement, it has in practice proven difficult for most data controllers. This is because the DPA does not set out specific periods for retaining personal data or give further guidance on what is meant by this Principle. The onus is therefore on organisations to determine what is 'necessary' in their own particular circumstances.

It is particularly important to comply with the Fifth Principle because failure to do so will most likely lead to a 'triple-whammy' failure of the Third, Fourth and Fifth Data Protection Principles. This is because holding personal data for longer than necessary will most likely also constitute holding excessive data and possibly also irrelevant and out of date data.

Conversely, retaining information in a planned and measured way should:

- increase staff and public confidence in your information handling processes;
- enable prompt document retrieval and reduce time responding to subject access requests;
- minimise the risk that your data are out of date or that they could be used in error or inadvertently destroyed or disclosed;
- reduce unnecessary time and resources updating data and holding data that you no longer need; and
- ensure you have a better chance of exploiting your information assets.

## How do I work out how long it is 'necessary' for my organisation to retain data?

Some organisations will need to keep certain types of personal data for longer than others. It is therefore impossible for the ICO to stipulate how long you should keep different categories of personal data for. But to help determine what is 'necessary' for your individual

Stephanie Pritchett runs PDP's Data Protection Essential Knowledge Level 2 course, where delegates can find out more about Data Retention and other areas of detailed data protection law compliance.

For further information or to make a booking please go to: [www.pdptraining.com/](http://www.pdptraining.com/)

organisation and to comply with best practice, it is recommended that you consider the following steps.

### 1. Carry out a Data Retention

**Audit or Review** — all data controllers need to put in place some form of procedure to delete data which are no longer required to fulfil the purposes for which they were originally collected, while also ensuring that important data are not being deleted prematurely.

All organisations need to regularly audit or review what personal data are being held by them both on-line and off-line.

As part of that review, you will also need to consider how long it is 'necessary' to retain data for. To do this, you will need to consider:

- *The needs of your individual organisation.* For what general business purposes were the personal data collected? For what purposes has the information actually been used by the organisation? Are there any other purposes for holding the personal data?
- *The current and future value of the information as well as the costs, risks and liabilities associated with retaining the information.* Are there any restrictions on keeping the personal data? Are there any regulatory requirements or professional rules requiring you

to keep the personal data? Are there other reasons why your business sector usually keeps this information for a certain length of time? Do you need to keep the information in case someone brings a claim against the organisation? If so, for how long? What are the limitation periods under statute?

- *The ease or difficulty of making sure it remains accurate and up to date.* How will you ensure

*statistical or research purposes.* The DPA states that personal data processed only for historical, statistical or research purposes in compliance with the conditions set out in section 33 may be kept indefinitely. Is there a value in your organisation to retaining the records for historical, statistical or research purposes? Are you sure the information will not be used in relation to decisions which affect particular individuals or in a manner likely to cause damage or distress? For how long will it be used for these purposes before it can then be deleted?

- *Information to be retained where relationships have ended.* When a business or employment relationship ends, you may need to keep some information but not all of it. You may need it in case a complaint is raised, a reference requested, a direct marketing request made, a tribunal action brought, etc. Other information, such as next of kin details, or an old addressee will most likely not be needed.
- *Information which needs to be kept because it is shared with another organisation.* What has been (or should be) agreed with the other organisation about how long the information is needed and what you should do with it when it is no longer needed? Should you ask the other organisation to return or delete information they are holding for you?

**2. Create or review your Data Retention Policy or Schedule** —The ICO expects larger organisations to carry out a data retention audit and then to draw up and adhere to a formal data retention schedule or policy.

If your organisation only holds a small amount of personal data, the ICO states that while you may not need a formal data retention policy, you will still need some procedures in place to ensure you can comply with

### ***“A data retention policy should usually set out:***

- *types of data processed (e.g. by organisation business function);*
- *the purpose(s) for processing the data (i.e. why the data are being kept);*
- *the maximum retention period for each type of data;*
- *where the data will be stored (e.g. archived, servers, personal folders etc);*
- *how data will be archived or destroyed when it no longer needs to be retained;*
- *how data will be kept secure in order to comply with the Seventh Principle; and*
- *who is in charge of the Data Retention Schedule (e.g. Compliance Officer or Data Protection Officer).”*

compliance with the other principles during the time you do keep the data? Will you archive the information or restrict access to it?

- *Any data to be kept for historical,*

*(Continued on page 12)*

(Continued from page 11)  
the Fifth Principle.

Even if you are not required to have one, a Data Retention Policy is a crucial part of an efficient and effective records management system. If it is properly developed and implemented, it can protect the interests of your organisation by ensuring that its records are kept for as long as they are needed to meet the operational needs of the organisation and to comply with legal and other requirements.

**3. Next steps** — Following your review, you will then need to ensure that your data retention policy or procedures are being complied with on a practical level and that your organisation is securely deleting, destroying, updating or archiving any information which it is no longer necessary for you to keep or which requires updating.

The need to do this was highlighted when Bord Gais was investigated by the Irish Data Protection Commissioner following the theft of four unencrypted laptops from its Dublin offices in June 2009. Amongst its other findings, that investigation noted that Bord Gais had breached the legislation by retaining personal data on the machines in question for longer than was justifiable.

## Conclusion

Remember that the onus is on your organisation to be able to justify what data retention periods and procedures you have in place and why you have the procedures that you do. Provided they are reasonable, your organisation will be in the best position to justify what periods it has set out in its procedures or policy.

This certainly seems to have borne out in *Chief Constable of Humberside Police & Ors v The Information Commissioner & Anor* [2009] EWCA Civ 1079, where in October 2009, the Court of Appeal overturned an earlier ICO and Information Tribunal decision that the retention by five police forces of a number of old minor criminal convictions records (relating to individuals convicted or cautioned on one occasion but not subsequently convicted of any other offences) was in

breach of the DPA and that the data should be deleted from the single central database on the Police National Computer.

The case hinged on the Third and Fifth Data Protection Principles (excessive data should not be kept and data should not be kept for longer than necessary). The Tribunal had ruled that the police did not need to retain the data if they were no longer required for their 'core' police operational purposes, and rejected evidence that this would include keeping information for use later by the Criminal Records Bureau, Crown Prosecution Service, and the courts.

The Court of Appeal, however, held that the ICO and the Tribunal's concepts of 'core purposes' were misconceived. While the police had to specify the purpose for which data were retained, there was no statutory constraint as to the purposes for which data could be retained except that the purposes had to be lawful to comply with the First Principle (fair and lawful processing).

The Court of Appeal said that the ICO had interfered too far in decisions that police forces alone should be making. In his ruling, Lord Justice Waller said "If the police say rationally and reasonably that convictions, however old or minor, have a value in the work they do that should, in effect, be the end of the matter".

The ICO was unsuccessful in its bid to appeal this case to the Supreme Court.

The Court of Appeal determined that the police were best placed to know how long their string was. If you have the proper procedures and schedules in place, then you will be well on track to having data retention all tied up.

---

**Stephanie Pritchett**

Pritchetts

stephanie@pritchettslaw.com

---