Deleting personal data

Data Protection Act

Please note: The following information has not been updated since the Data Protection Act 2018 became law. Although there may be some subtle differences between the guidance in this document and guidance reflecting the new law – we still consider the information useful to those in the media. This guidance will be updated soon to reflect the changes.

Contents

Introduction

The Data Protection Act 1998 (the DPA) is based around eight principles of good information handling. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

An overview of the main provisions of the DPA can be found in The Guide to Data Protection.

This is part of a series of guidance, which goes into more detail than the Guide, to help organisations to fully understand their obligations and promote good practice.

This guidance explains what organisations need to do to make sure they comply with the DPA when they archive or delete personal data.

Overview

- This guidance sets out how organisations can ensure compliance with the DPA, in particular the fifth data protection principle, when archiving or deleting personal information.
- It sets out what we mean by deletion, archiving and putting personal data 'beyond use'.

What the DPA says

The DPA does not define 'delete' or 'deletion' – but a plain English interpretation implies 'destruction'. In the days of paper records it was relatively easy to say whether information had been deleted or not, for example through incineration. The situation can be less certain with electronic storage, where information that has been 'deleted' may still exist, in some form or another, within an organisation's systems.

The deletion of personal data is an important activity in data protection, given the fifth data protection principle's requirement that "personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes".

In some cases an organisation may be required by law to delete an individual's personal data.

The ICO's Personal information online code of practice says:

> "It is good practice to make it clear to people what will happen to their information when they close their account – i.e. if it will be deleted irretrievably or simply deactivated or archived. Remember that if you do archive personal data, the rules of data protection, including subject access rights, still apply to it.
>
> If you offer users the option to delete personally identifiable information uploaded by them, the deletion must be real i.e. the content should not be recoverable in any way, for example, by accessing a URL from that site. It is bad practice to give a user the impression that a deletion is absolute, when in fact it is not."

Physical deletion or something else?

It is certainly the case that organisations should be absolutely clear with individuals about what they mean by deletion and what actually happens to personal data once they have deleted it.

This guidance is intended to counteract the problem of organisations informing people that their personal data has been deleted when, in fact, it is merely archived and could be re-instated.

It is also intended to encourage organisations to put safeguards in place for information that has been deleted but is still in fact in an organisation's possession. This guidance reflects our general line on deletion and will be relevant to all organisations that have to, or wish to, delete personal data.

Deletion and archiving

There is a significant difference between deleting information irretrievably, archiving it in a structured, retrievable manner or retaining it as random data in an un-emptied electronic wastebasket. Information that is archived, for example, is subject to the same data protection rules as 'live' information, although information that is in effect inert is far less likely to have any unfair or detrimental effect on an individual than live information.

However, the ICO will adopt a realistic approach in terms of recognising that deleting information from a system is not always a straightforward matter and that it is possible to put information 'beyond use', and for data protection compliance issues to be 'suspended' provided certain safeguards are in place:

- information has been deleted with no intention on the part of the data controller to use or access this again, but which may still exist in the electronic ether. For example, it could be waiting to be over-written with other data.
    - this information is no longer live. As such, data protection compliance issues are no longer applicable. (A parallel situation might be a bag of shredded paper waste. Although it may be possible to re-constitute the information from the fragments, this would be extremely difficult and it is unlikely that the organisation would have any intention of doing this.)
- information that should have been deleted but is in fact still held on a live system because, for technical reasons, it is not possible to delete this information without also deleting other information held in the same batch.
    - in cases like this the organisation holding the information may be prohibited by law from using it in the same way that it might use live information. This could happen if a court has ordered the deletion of information relating to a particular individual but this cannot be done without deleting information about other individuals held in the same batch.

Putting information 'beyond use'

The ICO will be satisfied that information has been 'put beyond use', if not actually deleted, provided that the data controller holding it:

- is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
- does not give any other organisation access to the personal data;
- surrounds the personal data with appropriate technical and organisational security; and
- commits to permanent deletion of the information if, or when, this becomes possible.

We will not require data controllers to grant individuals subject access to the personal data provided that all four safeguards above are in place. Nor will we take any action over compliance with the fifth data protection principle.

It is, however, important to note that where data put beyond use is still held it might need to be provided in response to a court order. Therefore data controllers should work towards technical solutions to prevent deletion problems recurring in the future.

Other considerations

Other relevant ICO guidance includes:

⇒ Deleting your data

More information

Additional guidance is available on our guidance pages if you need further information on other parts of the DPA.

This guidance has been developed drawing on ICO experience. Because of this it may provide more detail on issues that are often referred to the Information Commissioner than on those we rarely see. The guidance will be reviewed and considered from time to

time in line with new decisions of the Information Commissioner, Tribunals and courts.

It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

If you need any more information about this or any other aspect of data protection, please contact us, or visit our website at www.ico.org.uk.