# Fifth Data Protection Principle - Storage limitation

## At a glance

- You must not keep personal data for longer than you need it.
- You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
- You need a policy setting standard retention periods wherever possible, to comply with documentation requirements.
- You should also periodically review the data you hold, and erase or anonymize it when you no longer need it.
- You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
- You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

## Checklist

- We know what personal data we hold and why we need it.
- We carefully consider and can justify how long we keep personal data.
- We have a policy with standard retention periods where possible.
- We regularly review our information and erase or anonymize personal data when we no longer need it.
- We have appropriate processes in place to comply with individuals' requests for erasure under the right to stop or restrict processing.
- We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

## In brief

## What is the storage limitation principle?

The fifth data protection principle says:

Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

So, even if you collect and use personal data fairly and lawfully, you cannot keep it for longer than you actually need it.

There are close links here with the third (data minimization) and fourth (data accuracy) data protection principles.

The DPL does not set specific time limits for different types of data. This is up to you, and will depend on how long you need the data for your specified purposes, or how long you are required to maintain the data to comply with legal or regulatory requirements.

## Why is storage limitation important?

Ensuring that you erase or anonymize personal data when you no longer need it will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. Apart from helping you to comply with the data minimization and accuracy principles, this also reduces the risk that you will use such data in error – to the detriment of all concerned.

Personal data held for too long will, by definition, be unnecessary. You are unlikely to have a lawful basis for retention.

From a more practical perspective, it is inefficient to hold more personal data than you need, and there may be unnecessary costs associated with storage and security.

Remember that you must also respond to subject access requests for any personal data you hold. This may be more difficult if you are holding old data for longer than you need.

Good practice around storage limitation - with clear policies on retention periods and erasure - is also likely to reduce the burden of dealing with queries about retention and individual requests for erasure.

## Do you need a retention policy?

Retention policies or retention schedules list the types of record or information you hold, what you use them for, and how long you intend to keep them. They help you establish and document standard retention periods for different categories of personal data. See examples applicable in the Cayman Islands Government.

A retention schedule may form part of a broader 'information asset register' (IAR), or your personal data documentation.

It is best practice to establish and document standard retention periods for different categories of information you hold wherever possible. It is also advisable to have a system for ensuring that your organization keeps to these retention periods in practice, and for reviewing retention at appropriate intervals. Your policy must also be flexible enough to allow for early deletion if appropriate (for instance, in certain circumstance when an individual withdraws their consent or requires that you cease processing their data). If you are not actually using a record, you should reconsider whether you need to retain it.

If you are a small organization, do not keep large amounts of data or undertake only occasional low-risk processing, you may not need a documented retention policy.

However, if you don't have a retention policy (or if it doesn't cover all of the personal data you hold), you must still regularly review the data you hold, and delete or anonymize anything you no longer need.

## How should you set retention periods?

The DPL does not dictate how long you should keep personal data. It is up to you to justify this, based on your purposes for processing. You are in the best position to judge how long you need it. There may be other applicable statutory record retention requirements.

You must also be able to justify why you need to keep personal data in a form that permits identification of individuals. If you do not need to identify individuals, you should anonymize the data so that identification is no longer possible.

## Example

A bank holds personal data about its customers. This includes details of each customer's address, date of birth and mother's maiden name. The bank uses this information as part of its security procedures. It is appropriate for the bank to retain this data for as long as the customer has an account with the bank.

Even after the account has been closed, the bank may need to continue holding some of this information for legal or operational reasons for a set period.

### Example

A tracing agency holds personal data about a debtor so that it can find that individual on behalf of a creditor. Once it has found the individual and reported to the creditor, there may be no need to retain the information about the debtor – the agency should remove it from their systems unless there are good reasons for keeping it. Such reasons could include if the agency has also been asked to collect the debt, or because the agency is authorized to use the information to trace debtors on behalf of other creditors.

### Example

A bank may need to retain images from a CCTV system installed to prevent fraud at an ATM machine for several weeks, since a suspicious transaction may not come to light until the victim gets their bank statement. In contrast, a pub may only need to retain images from their CCTV system for a short period because incidents will come to light very quickly. However, if a crime is reported to the police, the pub will need to retain images until the police have time to collect them.

- You should consider your stated purposes for processing the personal data. You can keep it as long as one of those purposes still applies, but you should not keep data indefinitely 'just in case', or if there is only a small possibility that you will use it.
- You should consider whether you need to keep a record of a relationship with the individual once that relationship ends. You may not need to delete all personal data when the relationship ends. You may need to keep some information so that you can confirm that the relationship existed – and that it has ended – as well as some of its details.
- You should consider whether you need to keep information to defend possible future legal claims. However, you could still delete information that could not possibly be relevant to such a claim. Unless there is some other reason for keeping it, personal data should be deleted when such a claim could no longer arise.

### Example

An employer receives several applications for a job vacancy. Unless there is a clear business reason for doing so, the employer should not keep recruitment records for unsuccessful applicants beyond the statutory period in which a claim arising from the recruitment process may be brought.

## Example

An employer should review the personal data it holds about an employee when they leave the organization's employment. It will need to retain enough data to enable the organization to deal with, for example, providing references or pension arrangements. However, it should delete personal data that it is unlikely to need again from its records – such as the employee's emergency contact details, previous addresses, or beneficiary details.

## Example

A business receives a notice from a former customer requiring it to stop processing the customer's personal data for direct marketing. It is appropriate for the business to retain enough information about the former customer for it to stop including that person in future direct marketing activities.

- You should consider any legal or regulatory requirements. There are various legal requirements and professional guidelines about keeping certain kinds of records – such as information needed for audit purposes, or information on aspects of health and safety. For example, public authorities have to follow the National Archive and Public Records Law (2015 Revision) in retaining/disposing records, while entities which are regulated by the Cayman Islands Monetary Authority ("CIMA"), or which otherwise carry on "relevant financial business" for the purposes of compliance with anti-money laundering laws are required to keep data for specified periods. If you keep personal data to comply with an express legal requirement like these, you will not be considered to have kept the information for longer than necessary.
- You should consider any relevant industry standards or guidelines. For example, credit reference agencies may be permitted to keep consumer credit data for six years. Industry guidelines are a good starting point for standard retention periods and are likely to take a considered approach. However, they do not guarantee compliance. You must still be able to explain why those periods are justified, and keep them under review.

You must remember to take a proportionate approach, balancing your needs with the impact of retention on individuals' privacy. Don't forget that your retention of the data must also always be fair and meet legal conditions for processing.

## When should you review your retention?

You should review whether you still need personal data at the end of any standard retention period, and erase or anonymize it unless there is a clear justification for keeping it for longer. Automated systems can flag records for review, or delete information after a pre-determined period. This is particularly

useful if you hold many records of the same type.

It is also good practice to review your retention of personal data at regular intervals before this, especially if the standard retention period is lengthy or there is potential for a significant impact on individuals.

If you don't have a set retention period for the personal data, you must regularly review whether you still need it.

However, there is no firm rule about how regular these reviews must be. Your resources may be a relevant factor here, along with the privacy risk to individuals. The important thing to remember is that you must be able to justify your retention and how often you review it.

You must also review whether you still need personal data if the individual asks you to. Individuals have the absolute right to erasure of personal data that you no longer need for your specified purposes.

## What should you do with personal data you no longer need?

You can either erase (delete) it, or anonymize it.

You need to remember that there is a significant difference between permanently deleting personal data, and taking it offline. If personal data is stored offline, this should reduce its availability and the risk of misuse or mistake. However, you are still processing personal data. You should only store it offline (rather than delete it) if you can still justify holding it. You must be prepared to respond to subject access requests for personal data stored offline, and you must still comply with all the other principles and rights.

The word 'deletion' can mean different things in relation to electronic data, and it is not always possible to delete or erase all traces of the data. The key issue is to ensure you put the data beyond use. If it is appropriate to delete personal data from a live system, you should also delete it from any back-up of the information, subject to reasonability.

Alternatively, you can anonymize the data so that it is no longer "in a form which permits identification of data subjects".

Personal data that has been pseudonymized – e.g. key-coded – will usually still permit identification. Pseudonymization can be a useful tool for compliance with other principles such as data minimization and security – integrity and confidentiality, but the storage limitation principle still applies.

## Do we have to erase personal data from backup systems?

If a valid erasure request is received and no exemption applies then you will have to take steps to ensure erasure from backup systems as well as live systems. Those steps will depend on your particular circumstances, your retention schedule (particularly in regard to backups), and the technical mechanisms that are available to you.

You must be absolutely clear with individuals as to what will happen to their data when their erasure request is fulfilled, including in respect of backup systems.

It may be that the erasure request can be instantly fulfilled in your live systems, but that the data will remain within the backup environment for a certain period of time until it is overwritten.

The key issue is to put the backup data 'beyond use', even if it cannot be immediately overwritten. In any event. you must ensure, through technical and organizational measures, that you do not use the data within the backup for any other purpose, i.e. that the backup is simply held on your systems until it is replaced in line with an established schedule. Provided this is the case it may be unlikely that the retention of personal data within the backup would pose a significant risk, although this will depend on the specific context.

## How long can you keep personal data for archiving, research or statistical purposes?

Personal data processed for historical, statistical, or scientific purposes in compliance with the relevant conditions are exempt from the fifth data protection principle (storage limitation) to the extent to which compliance would be likely to prejudice those purposes.

You can keep personal data indefinitely if you are holding it only for those purposes. The general rule that you cannot hold personal data indefinitely 'just in case' does not apply if you are keeping it for these historical, research or statistical purposes.

You must have appropriate safeguards in place to protect individuals. For example, pseudonymization may be appropriate in some cases.

This must be your only purpose. If you justify indefinite retention on this basis, you cannot later use that data for another purpose - in particular for any decisions affecting particular individuals. This does not prevent other organizations from accessing public archives, but they must ensure their own collection and use of the personal data complies with the data protection principles.

## How does this apply to data sharing from controller to controller?

The DPL does not explicitly address this question. However, if you share personal data with other controllers, you have a duty to make reasonable efforts to ensure that the receiving controller will be compliant. The extent of efforts required will depend on the processing activity intended and the type of personal data being disclosed. Apart from that, it bears keeping in mind that you will need to have a legal basis for the disclosure of the personal data (as it is a processing itself), and the other controller will need to have a legal basis for their own processing.

As such, it is best practice to agree upfront on the handling of the shared data, especially for when you no longer need to share the data. In some cases, it may be best to return the shared data to the organization that supplied it without keeping a copy. In other cases, each of the organizations involved should delete their copies of the personal data.

### Example

Personal data about the customers of Company A is shared with Company B, compliant with all data protection principles. Company B is negotiating to buy Company A's business. The companies arrange for Company B to keep the information confidential, and use it only in connection with the proposed transaction. The sale does not go ahead and Company B returns the customer information to Company A without keeping a copy.

The organizations involved in an information-sharing initiative may each need to set their own retention periods, because some may have good reasons to retain personal data for longer than others. However, if each organization only holds the data for the purposes of the data-sharing initiative and it is no longer needed for that initiative, then all organizations with copies of the information should delete it.

## Relevant provisions

Data Protection Law, 2017

Schedule 1, part 1, paragraph 5: Fifth data protection principle – Storage limitation