

Introduction

One of the core principles of the UK GDPR is the storage limitation principle. This principle means that you must not keep personal data any longer than you need it. Article 5(1)(e) of the UK GDPR states that:

*1. Personal data shall be...
(e) kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed; where the personal data are processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) [which addresses safekeeping of data] technical and organizational measures shall be put in place to safeguard the rights and freedoms of the data subjects;*

As will be explained below, this does not mean that the data in question must be deleted or destroyed in its entirety. The data must be kept in a form which permits identification of data subjects¹, meaning that it cannot be properly pseudonymized.

In the context of a SME, it is unlikely that you will be retained on the grounds of public interest archiving, scientific or historical research purposes. Consequently, these guidance notes do not cover this aspect.

What will be most important from a data protection perspective is ensuring that you keep track of all personal data flowing in and out of your organization, such as customer information and employee data. You can or should keep this data in a form which permits identification of data subjects¹; for example, by reviewing retention regularly; and ensuring that you delete or otherwise rendering data *non-identifiable* in a timely manner. As will be explained below, this is particularly important and can have significant implications for your organization.

It must also be kept in mind that the data protection implications may extend beyond your own organization if you share personal data with other organizations. In such cases, agreeing suitable retention periods will be important and these will not necessarily be the same if each organization holding the personal data does so in a different manner.

¹“Data Protection Legislation” means a reference to the use of personal data and the privacy of personal data retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the “UK GDPR”), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2020 and the Privacy and Electronic Communications Regulations 2003 as amended.

Data Subject Rights

When considering data retention, in the Data Protection Legislation (and of the individual data subject may differ with.

Irrespective of your data retention the right to erasure, also known as the

Similarly, data subjects wishing to access request') must be provided that you hold about them, whether it

gations to abide by the principles of DPR), as detailed below, the rights always be respected and complied

Remember that if an individual exercises you must comply with this.

Access (by means of a 'data subject request' concerning the personal data held or not.

S

A

M

P

L

E

Part 1. Purpose and Lawful Basis

Before you can collect, hold, or process personal data at all, you must identify a proper lawful basis for doing so. You may, for example, have a lawful basis for processing personal data:

- With the consent of individual data subjects which you wish to use the personal data for;
- In order to enter into a contract with the individual prior to their request of the individual prior to their request;
- In order to fulfil a legal obligation (see above);
- To protect someone's vital interests;
- To perform a task with a clear public interest or in the exercise of official functions;
- In a manner consistent with the individual's own interests (this basis is the most restrictive).

Note that if you are collecting, holding, or processing special category personal data, additional criteria must be satisfied.

The lawful basis or bases upon which you collect, hold, and process personal data will be closely linked to the purpose or purposes for which you collect it. These purposes will, in turn, be linked to data retention as you may not be able to actually require it. Holding onto personal data for longer than the original purposes require.

Fairness should also be considered when you collect personal data will have upon the individual. You should only use the data in ways in which you can reasonably expect (or being able to explain and justify) and ensure you collect their personal data.

Transparency is also essential here when you collect personal data usage. It is important that individual data subjects are told about how you are processing of their personal data, in what ways, for what purposes, and - particularly relevant - how long you will keep it.

When deciding what personal data you collect, hold, and process, you should give thought to the purpose or purposes for which you collect it, linked to your lawful basis for processing it. This should be documented, as well as included in your privacy policy for individual data subjects.

It is also important to regularly review your purposes to ensure that you are still using personal data for a new purpose is compatible with the original purpose.

S

A

M

P

L

E

at all, you must identify a proper lawful basis for processing personal data:

- You must explain the specific purpose for which you wish to use the personal data and obtain the individual's consent;
- In order to enter into a contract with the individual prior to their request of the individual prior to their request;
- In order to fulfil a legal obligation (see above);
- To protect someone's vital interests;
- To perform a task with a clear public interest or in the exercise of official functions;
- In a manner consistent with the individual's own interests (this basis is the most restrictive).

Note that if you are collecting, holding, or processing special category personal data, additional criteria must be satisfied.

The lawful basis or bases upon which you collect, hold, and process personal data will be closely linked to the purpose or purposes for which you collect it. These purposes will, in turn, be linked to data retention as you may not be able to actually require it. Holding onto personal data for longer than the original purposes require.

Fairness should also be considered when you collect personal data will have upon the individual. You should only use the data in ways in which you can reasonably expect (or being able to explain and justify) and ensure you collect their personal data.

Transparency is also essential here when you collect personal data usage. It is important that individual data subjects are told about how you are processing of their personal data, in what ways, for what purposes, and - particularly relevant - how long you will keep it.

When deciding what personal data you collect, hold, and process, you should give thought to the purpose or purposes for which you collect it, linked to your lawful basis for processing it. This should be documented, as well as included in your privacy policy for individual data subjects.

It is also important to regularly review your purposes to ensure that you are still using personal data for a new purpose is compatible with the original purpose.

S

will either need specific consent or requires the new processing in the p in the SME context.

specific legal provision which allows or ground is clearly less likely to apply

Part 2. Data Minimization

A related principle set out in the U any personal data collected, held, a

minimization. You must ensure that

- Adequate in that it is sufficient to have collected it;
- Relevant in that it has a connection to that/those purpose or purposes; and
- Limited to what is necessary for purposes.

purpose or purposes for which you connection to that/those purpose or purposes.

It is important, therefore, to consider to be clear about why you need it. It is important to record these decisions so you can always come back and check your assumptions. A great care must be taken to ensure you are ultimately need.

will need at the very beginning and of data protection compliance, it is to demonstrate compliance and so that you can adapt to evolve as they progress, and to ensure you do not end up with more personal data than you

In particular, you should periodically review that you still need it. This connects your retention period in stone at the early stages of a project involving personal data is that your retention be.

data that you hold in order to ensure your data retention. Setting a retention period will rarely be sufficient. Just as your approach to data too should your approach to data

Part 3. Keeping Data Accurate

The requirement to keep personal data accurate which ties in closely with data retention is that the personal data you hold is correct and actively keeping data up-to-date.

te

Where any personal data is inaccurate you should quickly to correct it, erase it, or otherwise. An individual data subject's right to rectification of their data must also be handled with care.

er core principle of the UK GDPR, you should take all reasonable steps to make sure your data is accurate. In some cases, this will mean

The longer you keep personal data, the more likely the data protection principles enshrine that falling foul of one means you must take an interest not to keep personal data for

(out-of-date), you should take steps to ensure it remains accurate. It is also important to remember the importance of accuracy of personal data in everything.

remain accurate. The degree to which the UK GDPR and the Data Protection Legislation are interlinked means that they are not separate. It is, therefore, in your own best interests to ensure that your data is accurate and necessary.

A

M

P

L

E

Part 4. Storage Limitation

Thus far, these Guidance Notes cover data retention. When collecting, holding,

- Ensure that you have a lawful basis for processing the personal data in a fair and transparent manner;
- Collect the personal data only for those purposes that you have specified, and use that data only for those purposes that are compatible or you have another ground such as the public interest;
- Ensure that the personal data is kept for no longer than is actually necessary for your purposes;
- Keep the personal data in a secure form for no longer than is necessary in relation to the purposes for which the personal data are processed;
- Process the personal data in a secure manner.

It is the fourth point that will be our focus in this section.

As noted above, by only keeping personal data for as long as you need it, you are actively reducing the risks associated with data retention, particularly those associated with the holding of excessive data.

Furthermore, not only do longer retention periods increase the risk of non-compliance with the Data Protection Legislation, but they also increase the costs. Both physical and electronic data storage costs can add up unnecessarily, and complying with other data protection obligations such as responding to data subject access requests can become more burdensome, costly, and time-consuming.

The Data Retention Policy

One of the easiest ways to keep track of the key legal requirements relating to data retention is to use a Data Retention Policy. This policy should document every type of personal data collected, held, or processed by your organization, what you use that data for, the retention periods for that data, and the retention review periods, and other key information designed to help you determine whether or not you should still be holding the data in question.

Guidance from the Information Commissioner's Office (ICO) explains that small organizations undertaking low-risk personal data processing can have a documented data retention policy, however, it remains true that having a policy in place can make the process more efficient, and save time and money in the long run.

Data Retention Periods

In some cases, the retention period for personal data will be prescribed by law. Particular examples of this include tax and audit purposes, and other key compliance information. In countries where there may also be agreed

S

A

M

P

L

E

the *lead-up* to the issue of data retention. When collecting, holding, and processing the personal data, you must:

- Collect, hold, and process the personal data only for those purposes that are compatible or you have another ground such as the public interest;
- Ensure that the personal data is kept for no longer than is actually necessary for your purposes;
- Keep the personal data in a secure form for no longer than is necessary in relation to the purposes for which the personal data are processed;
- Process the personal data in a secure manner.

It is the fourth point that will be our focus in this section.

As noted above, by only keeping personal data for as long as you need it, you are actively reducing the risks associated with data retention, particularly those associated with the holding of excessive data.

Furthermore, not only do longer retention periods increase the risk of non-compliance with the Data Protection Legislation, but they also increase the costs. Both physical and electronic data storage costs can add up unnecessarily, and complying with other data protection obligations such as responding to data subject access requests can become more burdensome, costly, and time-consuming.

One of the easiest ways to keep track of the key legal requirements relating to data retention is to use a Data Retention Policy. This policy should document every type of personal data collected, held, or processed by your organization, what you use that data for, the retention periods for that data, and the retention review periods, and other key information designed to help you determine whether or not you should still be holding the data in question.

Guidance from the Information Commissioner's Office (ICO) explains that small organizations undertaking low-risk personal data processing can have a documented data retention policy, however, it remains true that having a policy in place can make the process more efficient, and save time and money in the long run.

In some cases, the retention period for personal data will be prescribed by law. Particular examples of this include tax and audit purposes, and other key compliance information. In countries where there may also be agreed

Not only should your review cover your data retention, but it should also refer back to your original purpose for holding, holding, and/or processing the personal data. You must carefully consider whether you can still legitimately rely upon your original justification.

Part 5. After the Retention Period

Once the retention period for personal data has expired, whether a review has determined that you should delete it earlier than planned, there are various options that are included for completeness and variety.

It is important to remember that data that is anonymized to the extent that it enables the identification of individual data subjects is still personal data. Therefore, you may not need to go through a full review, but you will need to strip those records of any identifying information that can identify individual data subjects once you no longer have a legitimate business purpose for the data to go to.

Similarly, some personal data can be anonymized; however, it is important to note that pseudonymization still enables identification in some circumstances. Under the UK GDPR, personal data is still personal data even if it does not directly identify someone if it can be combined with other data to do so.

Deletion or disposal will often be the preferred option. When deleting data stored electronically, it will be important to ensure that backups are also deleted.

Anonymizing Personal Data

If you do not wish to delete data records, you may wish to anonymize them; however, to ensure that the data is truly anonymized and cannot be subsequently combined with other data in order to identify individuals.

Two of the primary choices for anonymizing personal data are randomization and generalization. Randomization refers to the process of essentially removing the link between the data and the individual. Generalization involves aggregating individual data subjects. Aggregation (and could be applied, for example, to sales data) without identifying (or carrying) a great deal of risk of identifying individuals.

Once data has been anonymized, it is important to note that the very nature of the connections can be made to re-identify individuals.

It is important to note that the very nature of the processing. Consequently, the purpose for which you acquired the data in the first place unless you have another valid purpose for the data subjects.

S

A

M

P

L

E

your data retention, but it should also refer back to your original purpose for holding, holding, and/or processing the personal data. You must carefully consider whether you can still legitimately rely upon your original justification.

Once the retention period for personal data has expired, whether a review has determined that you should delete it earlier than planned, there are various options that are included for completeness and variety.

It is important to remember that data that is anonymized to the extent that it enables the identification of individual data subjects is still personal data. Therefore, you may not need to go through a full review, but you will need to strip those records of any identifying information that can identify individual data subjects once you no longer have a legitimate business purpose for the data to go to.

Similarly, some personal data can be anonymized; however, it is important to note that pseudonymization still enables identification in some circumstances. Under the UK GDPR, personal data is still personal data even if it does not directly identify someone if it can be combined with other data to do so.

Deletion or disposal will often be the preferred option. When deleting data stored electronically, it will be important to ensure that backups are also deleted.

If you do not wish to delete data records, you may wish to anonymize them; however, to ensure that the data is truly anonymized and cannot be subsequently combined with other data in order to identify individuals.

Two of the primary choices for anonymizing personal data are randomization and generalization. Randomization refers to the process of essentially removing the link between the data and the individual. Generalization involves aggregating individual data subjects. Aggregation (and could be applied, for example, to sales data) without identifying (or carrying) a great deal of risk of identifying individuals.

Once data has been anonymized, it is important to note that the very nature of the connections can be made to re-identify individuals.

It is important to note that the very nature of the processing. Consequently, the purpose for which you acquired the data in the first place unless you have another valid purpose for the data subjects.

S A M P L E

Clearly, then, the more permanent the data, the more you are expected to take an angle grinder to it. The Information Commissioner's Office (ICO) states:

*If you delete an item to your hard drive or perform a factory reset on a mobile device, data recovery experts can often retrieve it. However, data recovery experts say that **deletion is generally an adequate method of destroying personal data in most situations.***

In short, therefore, selecting the data to delete from your *Recycle Bin* or *Trash*, will generally be sufficient for most personal data. Nevertheless, if there are many specialist service providers

Disposing of Physical Records

While much information used in business is now stored electronically, more so in some contexts than others, in the past few decades, it is yet to become

With so much emphasis on secure electronic data, it is easy to overlook paper records; however, with electronic data, the same rules apply.

Even in cases where your primary focus is on electronic data, it is important to keep track of printed copies and their electronic counterparts are deleted. As part of your broader data protection and/or Data Security Policy.

When the retention period is up for physical records, they should be safely disposed of, taking care to avoid any damage. It is, therefore, logical to assume that shredding is sufficient. At the very least, physical

When selecting a suitable shredder, different levels of security are available, some in compliance with DIN standards. DIN 1 to 6 with 1 being the least secure and 6 being the most secure. Strips a maximum of 12mm wide at the end of the scale, DIN 6 shredders are generally used for government and financial institutions. Shredders are generally more suitable for home use if there is any doubt.

Retaining Personal Data for Archival

the better; however, you are not expected to use an angle grinder or microwave your USB sticks. As the ICO clearly states (emphasis added):

*'quick format' of your hard drive will be typically deleting data. However, data recovery experts say that **Even with that said, data deletion is generally an adequate method of destroying personal data from a device in most situations.***

Deleting it, and emptying your *Recycle Bin* or *Trash*, will generally be sufficient for most personal data. Nevertheless, if there are many specialist service providers

electronically, paper records still exist, and the transition of the paperless office over the

subsequent deletion, it can be easy to overlook paper records; however, with electronic data, the same rules apply.

Even in cases where your primary focus is on electronic data, it will be important to keep track of printed copies and their electronic counterparts are destroyed safely when their electronic counterparts are deleted. As part of your broader data protection and/or Data Security Policy.

When the retention period is up for physical records, any hardcopies of it should be safely disposed of, taking care to avoid any damage. It is, therefore, logical to assume that shredding is sufficient. At the very least, physical records should be shredded.

When selecting a suitable shredder, different levels of security are available, some in compliance with DIN standards. DIN 1 to 6 with 1 being the least secure and 6 being the most secure. Strips a maximum of 12mm wide at the end of the scale, DIN 6 shredders are generally used for government and financial institutions. Shredders are generally more suitable for home use if there is any doubt.

Retaining Personal Data for Archival

As noted above, in some cases, personal data indefinitely if you are in the public interest; scientific or historical research purposes.

Such data must still be protected including, if appropriate, pseudonymisation. It is important to stress that if personal data is retained on any of these grounds for a particular purpose, it must not be used subsequently for another purpose.

Part 6. Conclusions

The key to most areas of data protection is to have a clear track of personal data and your reasons for using it. This is particularly important when it comes to data retention. Without suitable records and data management systems, it is all too easy to hold onto personal data for far longer than it is needed. This is not only bad, but it could not affect anyone, but the longer data is kept, the more likely it is that it will be misused, lost, stolen, or even simply be rendered inaccurate by the passage of time.

Setting clear time limits for the retention of personal data and regularly reviewing those time limits is of paramount importance. It is important to avoid the trap of hanging onto data 'just in case' it could be used in the future.

A Data Retention Policy which records the personal data collected, held, and processed by your business, but also what is done with that data when you no longer need it. It is a valuable piece of documentation at both the practical level, and in demonstrating compliance with the principles of UK Data Protection Legislation.

S

A

M

P

L

E

protection law allows you to retain personal data indefinitely if you are in the public interest; scientific or historical research purposes.

Such data must still be protected including, if appropriate, pseudonymisation. It is important to stress that if personal data is retained on any of these grounds for a particular purpose, it must not be used subsequently for another purpose.

The key to most areas of data protection is to have a clear track of personal data and your reasons for using it. This is particularly important when it comes to data retention. Without suitable records and data management systems, it is all too easy to hold onto personal data for far longer than it is needed. This is not only bad, but it could not affect anyone, but the longer data is kept, the more likely it is that it will be misused, lost, stolen, or even simply be rendered inaccurate by the passage of time.

Setting clear time limits for the retention of personal data and regularly reviewing those time limits is of paramount importance. It is important to avoid the trap of hanging onto data 'just in case' it could be used in the future.

A Data Retention Policy which records the personal data collected, held, and processed by your business, but also what is done with that data when you no longer need it. It is a valuable piece of documentation at both the practical level, and in demonstrating compliance with the principles of UK Data Protection Legislation.