Data Retention Guidance

A practical guide for commercial and not-for-profit organisations

Publication date: 4th June 2020

Sponsored by exterro®

DPN
DATA PROTECTION NETWORK

This guidance is an initiative of the Data Protection Network. It has been made possible by contributions from Bristows LLP and representatives from a broad range of UK companies and not-for-profits. (Please see *Acknowledgements*)

This guidance should be read alongside official guidance from the European Data Protection Board (EDPB), the UK Information Commissioner's Office (ICO) and other Supervisory Authorities.

The information provided in this guidance represents the views of the Data Protection Network's Data Retention Working Group. It does not provide legal advice and cannot be interpreted as offering comprehensive guidance to the General Data Protection Regulation (Regulation (EU) 2016/679) or other statutory measures referred to in the document.

Copyright of Data Protection Network. All rights reserved. 2020 ©

Contents

Foreword

By Robert Bond, Partner at Bristows LLP and Chairman of the Data Protection Network

One of the core data protection principles is 'storage limitation' which requires organisations to retain personal data for only as long as it is necessary for the purposes it is held. A simple concept, but one which can present challenges for organisations to implement in practice. The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) provides specific requirements for the 'storage limitation' of personal data.

Article 5(1) says that personal data shall be...

> *(e) 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject* ***('storage limitation')****;'*

Article 25, which covers 'Data protection by design and by default' further requires that...

> *...'the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing,* ***the period of their storage*** *and their accessibility.'*

Before creating a data retention policy, organisations will need to fully understand what personal data they process and the purposes for which it is used. They then need to categorise data in a manner that works for the organisation, such as by function, data type or by country. Organisations can simplify this process by setting storage limitations from the start of any new or different personal data collection or new data solution. This approach puts storage limitation as an integral part of privacy by design.

When setting data retention periods, organisations need to consider other laws and statutory requirements relevant to the location of their processing operations and individuals. For example, a company may need to consider the laws of India if processing personal data in India.

Where there is no specific minimum or maximum legal retention period, organisations need to balance what retention period would be appropriate, necessary, and justifiable.

There are a number of factors to take into account in the decision-making process for retention periods. Decisions are likely to be more complex where personal data is processed for multiple purposes. For example, the data may no longer be necessary for one purpose but may remain necessary for another purpose.

Once retention periods are agreed, implementing a schedule across the business is often demanding. Due consideration needs to be given to what action to take when the retention period is reached – do you delete, destroy, pseudonymise or anonymise?

Purpose and scope

The purpose of this guidance is to provide a practical guide to help commercial and not-for-profit organisations overcome the challenges of meeting storage limitation obligations under data protection legislation.

This guidance provides a framework to help organisations navigate their way to making their own decisions in this area, taking into account their own processing requirements and the laws which apply to them.

The aim is for this guidance to apply to UK and European Union based organisations processing personal data for UK and EU citizens.

We have taken the view that it is not feasible to provide definitive guidance around retention schedules. This is due to significant variations in country-specific laws which may affect data retention periods (such as employment laws and local exemptions).

Alongside this guidance, if your organisation operates globally, you will need to consider other factors for different territories.

> ***"This guidance is principle-based, giving you the insight, considerations, framework, methodology and tools to enable your organisations to make educated decisions about appropriate personal data retention periods and how to implement these in practice."***

The guidance is primarily targeted at controllers who may process personal data in-house and / or also by outsourcing to processors.

We have included case studies to illustrate how others have approached different aspects of the data retention lifecycle.

However, processors who need to apply appropriate data retention periods on behalf of, and under the instruction of controllers, and take appropriate action when data reaches the end of its retention period, might also benefit from this guidance.

We identify key questions to ask when making decisions on data retention periods. We cover common purposes for processing, some sector-specific requirements and how to assess the necessity of retaining personal data where laws do not specify a time period.

The guidance includes the risks of over and under retention, as well as how to decide on the appropriate course of action when data retention periods have been reached.

We appreciate organisations will have different levels of maturity on data retention. We hope this guidance can help those whose data retention programmes are less developed, as well as supporting those who are looking to review their current practices.

1 The risks of over or under retention

Organisations need to be aware of the laws that apply to their personal data processing. Personal data must be kept long enough to comply with relevant legal obligations.

Laws may dictate minimum or maximum retention periods. In other scenarios laws may not specify retention periods and organisations will need to judge for themselves an appropriate retention period which they can justify.

What are the risks?

Organisations might expose themselves to risks if they keep personal data for longer than necessary, or indeed not keep it long enough.

1.1 Information security risks

Clearly the impact of a personal data breach could be significantly worse for an organisation which is keeping personal data for too long. For example:

- the volume of records involved in the breach may be larger and could affect far more individuals.
- if a regulator investigates and discovers certain data involved in the breach had been kept for longer than necessary, in breach of the law, enforcement action could be more likely and potentially more severe.
- damage to the organisation's reputation could be much greater.
- if the organisation is a processor acting on behalf of a controller, it may also face legal action from the controller.
- there could be more queries or class actions on behalf of the individuals who have been affected. It could raise complaints from individuals asking why their data has been kept so long.

1.2 Legal risks

Legally-defined data retention periods often exist to protect the interests of individuals. Where a law requires an organisation to keep personal data for a specific period, the organisation must keep relevant data at least long enough to meet these legal obligations.

If an organisation fails to keep records for the mandated period, it exposes itself to the risk that it may not be able to comply with the relevant laws and may also be undermining the interests of individuals.

1.3 Contractual or commercial risks

Certain personal data may need to be kept to meet contractual or commercial terms, such as:

- personal data collected as part of a sale, or to provide a service between an organisation and its customers.
- data required to substantiate guarantees, warranties, or ancillary products / services.
- data which is included within a contract between a data controller and its processor.

The associated risks in not keeping this data include responding to complaints or litigation from customers, or regulatory enforcement.

1.4 Customer expectations

Customers will expect organisations that process their personal data to respond to their needs, such as:

- answering customer service queries;
- responding to complaints; or
- changing their preferences.

In situations where there is no relevant law regarding the retention period for personal data, an organisation will still need to keep it for an appropriate period to meet its customers' reasonable expectations.

Equally once a customer contract ends, or lapses, a customer may not expect an organisation to hold their personal data any longer.

Appropriate retention periods must balance the interests and rights of each party.

1.5 Reputational risks

All the above risks could also result in reputational damage for an organisation which fails to meet its legal obligations, contractual obligations, or their customers' expectations.

2 Getting started

We recognise organisations may be at different stages of maturity with regard to data lifecycles and how long to keep personal data.

For those looking to develop data retention policies and good practices, the following flowchart sets out the key steps and considerations.

Data Retention Review Process

2.1 Where to start?

Organisations need to fully understand what personal data they process and the purposes for which that data is used. The first question is - Do you have all this information?

For example, have you:

- already mapped your dataflows; and
- logged all your personal data processing in your Record of Processing Activities (RoPA)?

Or

- Do you need to start this process?
- Perhaps you have some, but not all of the information you need?

If you do not fully understand what personal data you process and its purposes, how could you get this information?

- You could use your existing information sources - IT systems or information security information, existing data mapping, contracts with third parties, and so on.
- You could use data discovery software to mine your systems for personal dataflows. (You will still need to interpret the outputs, as they may not be in the form you need).
- You could engage with each function which processes personal data. For example, you may choose to run discovery workshops with key functions. This allows you to engage with them about data protection and understand more about their purposes for processing personal data.

Once you have the information you need, it is much easier to decide on or confirm the data retention period and to validate your Record of Processing Activity (RoPA) at the same time.

2.2 Categorise your data

The next step is to categorise personal data in a way that works best for the organisation.

For example, you could take one of the following approaches to categorising your data.

A - By individual type: employees, customers, prospects, business clients, and so on. If you are in healthcare, you may have patient special category data to consider. If you are a charity, you might have donor data, legacies data and data on individuals or families you support, which may include special category data.

B - By function: HR, Marketing, Operations, Finance, Procurement, and so on.

C - By country / region - Where do you operate from and where are individuals based? Perhaps you have an office, and / or customers located in the UK, Germany and Spain. If so, different local laws may apply, which may impact on retention periods.

3 Deciding on retention periods

Once you have identified and categorised your data, in a way that works for your organisation, you need to define appropriate data retention periods.

As your organisation may use personal data for multiple purposes, you need to take account of each specific purpose for processing, and the appropriate lawful basis for that processing, when considering an appropriate retention period.

In some circumstances a law will define a retention period, while in others organisations will need to make a balanced and justifiable decision on the period it judges to be necessary and appropriate.

In this guidance we have referenced certain important UK laws which affect data retention periods, but organisations must take account of laws in other territories, where applicable.

You need to assess the different types of personal data held within each category (personal data, special category data, anonymised data, pseudonymised data and so on).

3.1 Statutory requirement for retention

Where there is a legal or statutory requirement to keep personal data, you should use this to define your retention periods. For example, laws and obligations that might apply include the following.

- Data protection
- Intellectual property
- Statute of limitations
- The Companies Act
- Anti-money laundering
- Anti-bribery
- Modern slavery
- Clinical trial
- Litigation hold
- Medical devices
- Tax and employment laws (immigration laws)
- Government or Home Office rules
- Financial and insurance regulation

If there is no legal or statutory requirement, you need to make a justifiable judgement on how long to set your retention period for and document the logic behind it.

3.2 Duty to preserve documents for disclosure in UK legal proceedings

Once an organisation knows it is, or may become, a party to civil proceedings in the UK that either have or may be started (for example, where it has received a letter about this, or it intends to bring a counterclaim in existing proceedings), it is under various ongoing legal duties in relation to those potential proceedings. These duties are set out below and override other data retention rules set out elsewhere in this guidance.

A party to civil proceedings must therefore revisit its data retention in light of any actual or potential proceedings, to take account of these overriding duties. Note the term 'documents' as used in this context has a very wide meaning and will include, for example, video or audio material alongside material more commonly thought of as documents.

Ongoing duties include the following.

a. Taking reasonable steps to preserve documents in its control that may be relevant to any issue in the proceedings. This includes sending a 'written document preservation notice' to all its employees who may hold relevant documents and taking reasonable steps to make sure any third parties who may hold relevant documents do not destroy them.
b. Once proceedings have been started, to disclose relevant documents, including those adverse to its case, unless privileged (see below).
c. Complying with any disclosure order from the court.
d. Searching for documents in a responsible and conscientious manner to meet the stated purpose of the search.
e. Acting honestly when disclosing documents and reviewing documents disclosed by the other party.
f. Using reasonable efforts to avoid providing documents to another party that are not relevant to the issues in the proceedings.

There may be other rules relating to documents that are commercially sensitive and / or confidential, which are beyond the scope of this guidance.

3.3 How do you know what's 'necessary'?

Where there is no statutory requirement, organisations need to ask their internal data owners and / or relevant function heads questions about what data is 'necessary' for the organisation to keep.

Consider the following questions.

a. Are there any industry standards, guidelines or known good-practice guidelines?
b. Does the product lifecycle or approach to pricing have an effect on retention?
c. What are the business drivers for retention? Are they justifiable?
d. What evidence is there that certain data is needed for the proposed amount of time?
e. Is there potential for litigation?
f. Could you identify or develop use cases for personal data and have the business validate them?
g. Is it necessary to keep personal data to handle complaints?
h. Is a customer issue likely to require data to be retained? For example, in recent years PPI claims in the UK.

We recognise many organisations may process similar categories of data. We have therefore provided more detailed considerations and created some example templates to help you.

These can all be found in *Appendix A* and include the following.

Company records
Employee records
Health and safety and environmental records
Children's records
Medical records
Clinical trial records
Finance, accounting and tax records
Insurance records
Customer contract records
Marketing records
Public domain records
Data used for or created by artificial intelligence (AI)
Archived records

The above list is not exhaustive. While these examples are based on UK law, we hope they might provide pointers for those who need to account for the laws, regulation and best practice in other territories.

4 Controllers, processors and sub-processors

Organisations who use suppliers (who are acting as processors) need to make sure there are clear contractual instructions for data retention. These should include specific actions to take when a retention period ends.

Processors must make sure they can implement these instructions promptly and need to consider data retention when outsourcing data tasks to sub-processors.

Joint controllers have a duty to jointly determine how long the personal data they both control should be kept and what action to take at the end of that period.

There should be clear documented evidence of an action to delete personal data, particularly if done externally by a processor. For example, a data destruction certificate.

4.1 Controller obligations

The following table sets out a controller's data retention obligations. Joint controllers should make sure the responsibilities outlined below are practical and clear in any contract.

Controller obligations	
Storage limitation principle	Keep personal data for only as long as it is necessary for the purposes it is needed.
Policy and schedule	Make sure you have a data retention policy and a schedule which sets out your standard retention periods. Make sure your policies and practices include both paper and electronic personal data.
Categorisation	Make sure you consider **all** categories of personal data in your retention schedule.
Record of Processing Activities (RoPA)	Make sure your RoPA includes, or is linked to, your retention schedule for the different categories of personal data you process. Include a reference to the basis on which you determined the retention schedule. For example, based on internal policies, or on industry guidelines. (Note some organisations are not required to maintain a RoPA.)
Roles and responsibilities	Make sure you have a clearly defined and enforced set of data roles and responsibilities for personal data governance, including data retention.
Justification	You must be able to justify how long you keep personal data and document this reasoning.
Review	Regularly review the data you hold, and its retention periods. Delete or anonymise data which has reached or passed its retention period.

Continued

Controller obligations	
Handling challenges to retention	Consider any potential challenges to your retention decisions. Individuals have a 'right to erasure' which may apply if you no longer need to keep their personal data.
Archiving	You can keep personal data longer for public interest archiving, scientific or historical research, or statistical purposes.
Transparency and right to be informed	Make sure you provide individuals with clear information about your data retention practices.
Limitation	Implement processes to make sure the personal data you keep remains accurate, adequate, relevant and not excessive.
Information security	Make sure you apply high levels of information security to protect personal data, particularly regarding special categories of personal data and children's data.
Data subject rights	Make sure staff fully understand your data retention policy so they can manage expectations, particularly for individual rights requests, (including but not limited to subject access, correction, erasure, marketing opt-outs and data portability).
Backed-up / archive data stores	Make sure you apply the same principles of governance and control to backups and data archives.
Physical data retention and storage	Make sure you cover full end-to-end processes with both planned and unscheduled tests of access to, and security of, personal data, including both active and archived data.
Adoption of data pseudonymisation / anonymisation	Make sure you consider your processors' expectations (if any) and how you apply anonymisation or pseudonymisation principles internally.
Processor contracts	Make sure there is a written contract with your processors which references requirements and accountabilities for data retention, and contains or links to your data retention principles, practices and periods.
Contract terms	Make sure contractual clauses cover the processor's responsibility for any actions of sub-processors. Make sure there are clear terms for end of contract destruction, removal or transfer of data, including evidence.
Contract execution	Carry out appropriate monitoring of processors to make sure they are fulfilling their stated contractual obligations.
Contract termination	Request evidence that data has been removed / destroyed in line with the contract terms.

4.2 Processor obligations

A processor is responsible for keeping personal data in line with the controller's instructions. The following table sets out processor and sub-processor responsibilities.

Processor and sub-processor obligations

	Processor	Sub-processor
Adoption of data pseudonymisation or anonymisation	Make sure you can fully and accurately carry out any data controller requirements to anonymise or pseudonymise personal data. Make sure any sub-processors can also fully and accurately execute any requirements.	Make sure you can fully and accurately carry out any data controller requirements to anonymise or pseudonymise personal data.
Contract	Make sure there is a written contract which references requirements and accountabilities for data retention.	Same as for processors.
Contract terms	Make sure any relevant conditions imposed by the controller are passed on to sub-processors and included in any contract terms. Consider additional legal or other obligations which may require the processor to keep the data beyond termination or standard deletion periods. For example, for auditing requirements.	Take appropriate steps to make sure the processor has the contractual right to subcontract.
Contract execution	Carry out appropriate monitoring of sub-processors to make sure they are fulfilling their stated contract obligations. Make sure you can provide acceptable evidence about full data removal throughout the term of the contract.	
Contract termination	Make sure you can provide acceptable evidence about full data removal at the end of the contract.	Same as for processors.

5 Creating a data retention policy and schedule

Top tips for creating a successful data retention policy and schedule.

Simple is better when creating your policy. Start small and ramp up as your needs change. Employees have a lot to do and are more likely to comply with a simple policy and schedule.

Communicate while you are developing your policy. Engage others across the organisation at all levels. You will need organisational buy-in to implement the policy and schedule you create. Once done, let people know they exist and what they need to do to comply with them.

Gather feedback – ask individuals impacted by the policy and schedule how this has affected them and use their input to continually improve them.

Notify relevant business owners when a retention period is reached to confirm the decision.

5.1 Creating an organisational policy for data retention

Organisations should set a policy that provides guidance to staff and contractors on data retention principles and practices, and how to apply them.

A policy should describe the organisation's approach to keeping personal data for only as long as it is necessary for the purposes it is held.

Much of what you will need to do to tailor your policy to meet organisational needs will be specific to your industry or sector. However, there are some basic steps that everyone can follow which will help build a policy that is easy to follow, maintain and update.

Involve people across your organisation

By involving a cross-section of individuals in the organisation, you will be able to make sure you have considered all types of personal data and the range of purposes relevant to data retention.

This might include people from your legal, finance, technology and other teams including managers and supervisors who have specialist knowledge on their areas of the business.

Others will be able to flag up situations you may not be aware of, for instance, personal data shared with a new supplier, or a new data collection point.

In addition to making sure you don't miss something important you can use this as an opportunity to engage others, creating the buy-in needed to make implementation easier.

Understand the laws and regulations that apply to your organisation

You will have both legal and commercial reasons to keep information and it's important to strike the right balance between each of these.

Your organisation may have commercial requirements for data retention such as contract obligations, sector-specific rules, administrative or operational requirements relating to daily functions.

Your data retention policy must allow you to sufficiently maintain business as usual. By identifying the laws, regulations, codes of practice and business-specific considerations relevant to your organisation you can consider data retention holistically.

Compose your policy

Some organisations may adopt a holistic 'Data Management Policy' covering the whole lifecycle of data from creation to destruction. Others may adopt separate but linked policies for certain key data life stages, from data collection to retention.

Some organisations find it helpful to refer to a 'Data Retention' or 'Records Management Policy' template which provides a basic framework to follow.

Your policy will include information about your organisation's approach to data retention. There are different approaches. While some organisations choose to include the specific retention periods for each type of data, these can become very detailed, so many organisations prefer to set these out in a separate data retention schedule.

Your policy will be specific to your organisation, but here are some of the sections you might want to include.

- Purpose, scope and who the policy applies to. This could include those outside the direct organisation, for example, third parties and processors.
- Key definitions describing the terms you use and what they mean.
- Regulatory or sector-specific requirements, including data protection law.
- The organisation's approach to data retention – general principles, practices and responsibilities.
- Specific team duties or responsibilities.
- Practical guidance for those who manage data and need to comply with the policy, including what should happen when the retention period is reached.
- Links or appendices, including where to find the current data retention schedule if this is separate to the policy.
- Date published, version number, when it is due for review.
- Owner(s) of the policy and contact details for questions.

Communicate the policy across the organisation, and if relevant to third parties / partners

Once done, you need to communicate the policy to staff and help them understand what it means for them. Awareness is key for successful implementation.

5.2 Creating a data retention schedule

A data retention schedule defines how long to keep data items by setting either minimum or maximum retention periods. It provides guidelines on what to do with the data when these periods come to an end.

This will often lead to destroying the personal data but there are other options such as archiving, anonymisation or putting the data 'beyond use'. These options are explored in *Section 6*.

Data retention schedules are designed to help maintain governance and regulatory compliance but as data volumes continue to grow, they can also help reduce records management and storage costs by getting rid of data no longer relevant to business processes.

> **“Remember, keeping and using data has a cost. It is better to delete it when you do not need it.”**

The layout and contents of the schedule will vary between different organisations but will generally include the following.

- Information about how the organisation has classified its data, such as by geographic region, by function, and so on.
- A description of each dataset.
- Minimum / maximum retention periods.
- The rationale for the retention decision, for example, legal requirement, commercial reasons and so on.
- The action required when the retention period is reached.

5.3 Other considerations

Transparency

Data protection law requires organisations to be transparent about their retention periods.

GDPR Article 13(2)(a) specifically requires that at the time personal data is collected there should be information about, ‘the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period’.

Alignment with other requirements

The GDPR and the UK Data Protection Act 2018 have a number of requirements which compliment your data retention policy. Specifically, the GDPR requirement to maintain a Record of Processing Activities (RoPA) and the Data Protection Act 2018 requirement for appropriate policy documents when processing certain types of special category data.

Although not necessarily relevant to all organisations or all personal data, you should consider whether you need to merge, cross-reference, or link your data retention schedule to these other documents.

Whatever you decide, a common approach will help maintain the integrity of the information.

6 Action when the retention period is reached

Organisations need to decide in advance on the right course of action once the data is no longer required for the specified purposes, or the agreed retention period is reached.

In summary, you should do the following.

- Identify the relevant records.
- Notify the relevant business owner to confirm the retention decision.
- Consider any changes to circumstances.
- Make sure the business / risk owner makes the decision to either:
  - delete digital records including backup
  - pseudonymise
  - anonymise
  - destroy physical records, such as shred, incinerate and so on.
- Document the decision and keep evidence of the action.
- Repeat for next the batch of records.

6.1 Identify relevant records

The first step is to identify the records in scope. The most common scenarios which should trigger an action are that:

a. the retention period for a specified purpose has passed.
b. you were required by law to delete the data after a certain date.
c. you have identified that you no longer need to keep the data.
d. you have received an objection to processing based on GDPR Article 6(1)(e) 'legitimate interest' and there is no overriding reason to keep the personal data.

6.2 Notify and consider any changes

Once you have identified the records, it's advisable to contact the relevant business owner to confirm the retention decision and consider any potential changes in circumstances. This could have an impact on your decision to delete or not.

6.3 What's the right course of action?

You must then consider the right course of action. There are several options depending on how you hold the personal data, however, in each case, you need a process for demonstrating compliance.

Demonstrating compliance may mean implementing an appropriate policy and procedure for managing how you get rid of personal data.

By complying with the data minimisation principle, by keeping data for a legitimate purpose but stopping processing it for redundant purposes, you'll make sure there's less data to sort through.

With regards to documenting your decisions, organisations may consider aligning themselves to the practices below, or accrediting to certain standards such as ISO27001 or BS10012.

Options when a retention period is reached

There are several different approaches organisations could take when the data retention period is reached, for example:

- deletion
- pseudonymisation
- anonymisation
- disposal, including shredding

You will also want to make sure deletion does not adversely affect key processes in your organisation, such as reporting, algorithms and other programmes. For this reason, you may wish to pseudonymise or anonymise your data.

Pseudonymise or anonymise?

Many organisations want to get value from their digital assets. Being able to find and use the wealth of information while removing personal data is an attractive proposition. However, anonymisation and pseudonymisation present different approaches.

Pseudonymise?

Pseudonymisation is a process which substitutes information in a dataset that identifies an individual with an artificial identifier or pseudonym. You then need extra information to re-identify the individual. This process reduces risks to individuals.

The GDPR defines pseudonymisation as:

> **"...the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."**

Importantly, pseudonymous data is still personal data. GDPR recital 26 is clear that pseudonymous data which could be linked to a natural person by using extra information is information relating to an identifiable natural person.

Consequently, pseudonymising records would not remove GDPR obligations on retention. You should consider other options.

Anonymise?

Anonymisation is process of removing all information which identifies a living person so the data can no longer be linked back to a unique individual. The GDPR does not apply to anonymised information. Recital 26 of the GDPR explains that:

> **"...The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."**

However, the ICO highlights that you should be careful when attempting to anonymise information. For the information to be truly anonymised, you should not be able to re-identify an individual. If you could, at any point, use any reasonably available means to re-identify the individuals, you will not have effectively anonymised that data, but you will have pseudonymised it, which means it is still personal data.

A previous decision[1] by the Austrian Supervisory Authority stated that anonymising was sufficient for the deletion right as the information was no longer 'personal data.' ICO guidance includes the following question and response:

> **"What should we do with personal data that we no longer need?"**
> **"You can either erase (delete) it, or anonymise it.[2]"**

Therefore, taking this action for retention would remove the data retention risk to personal data and remove your GDPR obligation, as long as the information is truly anonymised.

Deletion

As well as physical records, you also need to take action on your digital records.

There are software methods of clearing data, such as using zeros and ones to overwrite data. This makes the data unrecoverable.

This process should include backup copies of data. The ICO states that, '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 [3]'.

Personal data may be instantly deleted from live systems. However, personal data may still remain in backups, until it is overwritten. If the backup data cannot be immediately overwritten it must be put 'beyond use'. This means you must make sure the data is not used for any other purpose and is simply held on your systems until it is replaced in line with an established schedule.

1 5 December 2018, DSB-D123.270/0009-DSB/2018

2 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/

3 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/

Examples of circumstances where data may be put 'beyond use' are as follows.

- Information may have been deleted but not yet overwritten.
- Information should have been deleted but it is not possible to do so without also deleting other information held in the same batch[4].

The ICO (for example) will be satisfied that information is 'beyond use' if the data controller:

- is not able, or will not attempt, to use the personal data to inform any decision about any individual or in a way that affects them;
- does not give any other organisation access to the personal data;
- has in place appropriate technical and organisational security; and
- commits to permanently deleting the information if, or when, this becomes possible.

Unstructured data

The retention period will also apply to unstructured data which contains personal data. The most common type is electronic communications such as emails, instant messaging, files and other documents. Unstructured data may be in many different formats and systems, such as Microsoft Exchange.

You will need to be able to analyse the unstructured data to find any personal data stored there so you can delete it in line with your retention schedules, any deletion request or statutory limit. Depending on the size of your organisation, you may need to use dedicated tools to analyse the content of unstructured data.

Destruction of physical records

Destruction is an important part of the lifecycle of physical records. It is likely to be the best action for physical records when the organisation no longer needs the data and does not need to hold data in a pseudonymised or anonymised format (such as for historical analysis purposes).

Destruction is the final action for about 95% of most organisations' physical records. Physical destruction may include shredding, pulping or burning paper records.

As part of accountability requirements, controllers should document the disposal decision in disposal policies or schedules.

Many organisations use third-party processors to get rid of their data. Benefits include reducing in-house storage costs, server space or machinery. However, there are risks and obligations under the GDPR, such as the obligation to have an appropriate data protection agreement with the processor(s).

Alternatively, some organisations get rid of data remotely following an agreed process. For instance, a processor providing daily, weekly or monthly batch notifications and destroying archived information in line with documented retention dates. In either case, it is important to identify records and when they are due to be deleted.

The ICO refers[5] to the National Archives as an example of good records management for getting rid of records. The National Archives have the following examples for disposal classes[6].

4 https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf

5 ICO refers to National Archives in their Guidance:

6 National Archives, Guide 8 'Destruction of Records' https://www.nationalarchives.gov.uk/documents/information-management/rm-code-guide8.pdf page 6.

Example: disposal classes

- **Personnel files –** each file refers to a different member of staff, but the file structure and contents will be identical to the other files in the set. You can therefore set a retention period for all files in the set.
- **Complaints records –** the nature of the complaint may differ, but handling will follow an agreed process, and most complaints files can have the same retention period.
- **Project records –** if the organisation uses a standard project methodology, they will create the same types of records during each project, such as project plans, reports, and so on.
- **Procurement records –** if the organisation has standard procurement rules, they will create the same types of records during procurement, for example, statement of requirements, business case, invitations to tender, and so on.

7 Implementation of data retention periods

Once you are ready to implement agreed retention periods you should consider these key topics.

7.1 People and process challenges: winning hearts and minds

- Consider how to get senior leadership support.
- You will need to confirm who makes the final decision on data retention periods and who supports them to implement these periods.
- Consult with your stakeholders and agree the best approach.
- Try to adopt a flexible approach as things change.
- Internal awareness – consider how best to communicate your data retention policy and schedule across the teams who manage personal data and the technology teams who will support them with the systems.
- External transparency - consider how to notify your customers / clients / supporters about how long you will keep their data, for example, in your privacy notices. How much detail will you give about specific retention periods?

You will need to build strong relationships with data owners, but also with your technology team - particularly those who are responsible for the IT systems which hold the data.

To encourage people to help you to implement successfully, you will need to build strong relationships with your stakeholders. Help your colleagues understand data retention and how you have made decisions.

You will need to be able to clearly state the benefits of implementing data retention policies and practices, so that data retention becomes part of a wider topic of **'How do I use this information to drive my business forward'**.

7.2 Technology challenges

You could face some real challenges when attempting to roll out the data retention policy and schedule, for example:

- legacy systems may be inflexible and sometimes they have limited data destruction capabilities.
- decommissioned systems, or systems due for decommission, may still hold personal data which will need to be destroyed.
- data held on backups.
- business continuity risks (such as if you need to restore data which has been deleted).

7.3 Monitoring your data so you know when it reaches its retention period

You may wish to consider whether it is possible to 'tag' the data in your systems for retention purposes.

When you collect data, you will have specific purposes for keeping that data. You will know your main purpose, which should have its own retention period, and you may also have secondary purposes which have their own retention periods.

You may wish to tag the data with an expected retention period (or date) based on these purposes and update the tags as and when processing changes. Later you can look at those tags and ask these questions.

- Do they still apply?
- Do I still need this data?
- Do I need to change it?

At that stage you have a history, you can see how you have been processing it and make an informed decision.

Where there is a statutory requirement to keep personal data, take this into account when setting the retention period and setting tags.

7.4 Backups of personal data

Every organisation and its backup methodologies are unique, consequently, each organisation must implement data retention and deletion procedures for backups that are specific to its own circumstances.

The GDPR principles and obligations apply to backup or archived personal data the same way as they do to 'live' data.

As well as GDPR's storage limitation principle it also requires disaster recovery (Article 32(1)(c)).

If there is a disaster, an organisation must make sure it can quickly restore personal data from backups and provide access to the personal data to an organisation's staff or individuals. A comprehensive business continuity plan is likely to be the best way to achieve this.

How do you apply your retention policy to this backup data?

Where multiple data sets (for example, for various business functions) are backed up together in batches, it may be difficult or impossible in practice to delete certain or specific files from backup.

In this situation an organisation's standard data retention policy may not be feasible for backups, as this architecture may prevent an organisation from searching the backup file to delete a certain file(s) without having to restore the whole backup. Therefore, it is likely that these files will need to be overwritten or deleted in batches.

Putting data 'beyond use'

Several Data Protection Authorities, including the ICO and CNIL[7] , have provided practical guidance on personal data in a backup. These provide useful flexibility for organisations. The ICO stated in its 2012[8] guidance that where personal data is held electronically which cannot be deleted in line with a retention policy due to technical reasons, it could instead be put 'beyond use' and 'suspended' from data protection compliance issues.

A controller or processor can put personal data 'beyond use' provided the organisation holding it:

- is not able, or will not attempt, to use the personal data to inform any decision about any individual or in a way that affects them;
- does not give any other organisation access to the personal data;
- has in place appropriate technical and organisational security; and
- commits to permanently deleting the information if, or when, this becomes possible.

An organisation should make sure a limited set number of individuals and organisations are able to access backups, in case they need to restore the data. This will prevent an employee or a processor from accidentally attempting to use personal data that should be 'inactive'.

An organisation should also make sure the personal data is securely stored and, in certain situations, pseudonymised or aggregated. The ICO has also clearly indicated that an organisation cannot backup the data and then ignore it - organisations still need some permanent deletion process.

If personal data cannot be deleted from backup except on a rolling basis, for example, where it's technically unfeasible, the organisation should document it internally along with other information, such as the security protocols protecting the data on backups.

Processor backups

Data processors can only act on the instructions of the controller. This implies that they must delete the personal data in line with the controller's instructions, their data processing agreement with the controller or at the end of the contract.

However, processors also need to keep personal data in backups. Processors should clearly state in their agreements with the controller their procedures for deletion requests and getting rid of personal data within backups.

7 On January 26, 2018, Stéphane Estevez blogged the he received guidance from the CNIL stating that organisations do not need to delete data from backups when receiving a data subject request. This guidance can likely be applied to data retention standards as well. Organisations will have to clearly explain to the data subject (using clear and plain language) that his or her personal data has been removed from production systems, but a backup copy may remain, but will expire after a certain amount of time (indicate the retention time in your communication with the data subject). See, *https://blog.quantum.com/backup-administrators-the-1-advice-to-deal-with-gdpr-and-the-right-of-erasure/.*

8 See, *https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf* Similarly, the Danish Data Protection authorities also indicated that organisations do not have to delete personal data from backup where it is not technically possible. See: *https://www.datatilsynet.dk/emner/persondatasikkerhed/sletning/*

8 Ongoing oversight of data retention

Once you have set up your data retention policy and implemented the data retention periods, you will still need ongoing governance to properly manage ongoing changes, such as new processing, changes to existing processing and the legal framework affecting your data retention periods.

You may wish to create a forum where key stakeholders can come together to review ongoing processing changes and evaluate requests for different retention periods, for anonymisation or for deletion. It may also be helpful to train people in your business functions so they can identify retention issues.

9 Case studies

Case study A – a charity

Established in 1867, Barnardo's works to transform the lives of the most vulnerable children across the UK. Once famous for its care homes, the charity now supports over 300,000 children annually in a variety of settings, including fostering and adoption.

Barnardo's has an archive which dates from the earliest children coming into the homes in 1870. Many of the records are kept because we have a legal requirement to hold them, some are kept because we feel we have a moral obligation to provide information to the descendants of those we cared for.

As a UK-wide organisation Barnardo's has to consider retention across all four nations, which means the length of time we have to keep the data for looked-after children and their carers may differ from nation to nation. This obviously makes storing and getting rid of information more complex. For example, the law requires us to keep data for a child fostered in England for 75 years, but if they are looked after in Scotland, we keep it for 100 years.

As well as legal requirements, it's important for organisations to be aware of external factors that are beyond their control which may affect retention periods. The Independent Inquiry into Child Sexual Abuse (IICSA) in England and Wales was set up to examine how the country's institutions handled their duty of care to protect children from sexual abuse. Announced by the then Home Secretary, Theresa May, on 7 July 2014, IICSA has had a significant impact on retention periods for all organisations that work with children. As a result, those organisations are advised to keep data until the end of the inquiry (whenever that may be) in case it is required. For Barnardo's this means that some records are currently being kept beyond their defined retention date which requires a change of process and procedure.

The archive meets the needs of former residents and their families by allowing access to records, and providing support, through the difficult process of receiving what might be painful or confusing information. On average Barnardo's receives 3,000 enquiries a year, half of which are family history enquiries and the rest are subject access requests from former care adults and those receiving services today.

Although having a formal retention schedule is crucial to the success of responding to enquiries from a variety of audiences, a good retention schedule can also help provide a narrative to the past from a social care perspective. The records help us to understand all variations of the experience of being in care, and how important it is to learn, question and improve the way we support and protect children today.

Case study B – a travel business

A group of companies in the travel sector trades in several countries, with their main operational centres spread across the EU.

When reviewing their Group data retention policy, the business chose to focus on defining specific retention periods by region for each of their EU markets. They took the opportunity to define retention periods relating to both personal data and non-personal data at the same time.

The Privacy team developed a template for a group data retention schedule containing standard data attributes and descriptions, such as accounting and finance records, employment records, marketing and sales records, and so on.

The Legal, Privacy and Business teams in each market then completed their own data retention schedule using this template, defining their own retention periods with reference to local laws, regulations and local trading practices and standards. They also provided their business justification for each retention period.

Once created, the Group data retention schedule needed to be implemented, with the help of local technology teams. Personal data should be routinely destroyed but there must be the capability to suspend or override this to keep data, for example, for a legal hold.

Local project teams checked, reviewed and implemented their local data retention schedule. Given the large number of systems which held data, the business recognised the scale of the challenges, including timescales. They encouraged markets to take a risk-based approach and prioritise any necessary work based on, for example, the type and volume of data, business requirements and risk of harm or damage if a system was compromised or over-retaining data.

Later, the Group Audit team assessed the data protection compliance of key markets and businesses. Data retention is one of the key compliance controls they assess.

Case study C – a construction and infrastructure business

A construction and infrastructure sector multinational has operations across multiple jurisdictions in Europe, Asia and the Americas.

When reviewing our records management and retention policies, the business was aware that local law and regulatory requirements differed significantly in the different territories. The approach was to establish a record management policy for UK headquarter operations with overseas entities adopting their own retention policies.

At the UK headquarter level, with advice from external counsel, the business created a records management policy setting out principles on good record management and defining recommended retention periods for different data categories (such as electronic and physical) on a non-exhaustive basis.

The policy considered relevant operational, legal, regulatory and accountability requirements likely to apply to our sector. In the UK construction sector, most client projects involve long-term contracts executed as deeds which have a 12-year limitation period for claims, as well as post-completion defects liability periods. Any retention policy had to acknowledge that project records may be required for legal, contractual, or regulatory compliance purposes for up to 12 years after the project ended.

Health and safety records are also a priority for the construction industry. The policy had to include appropriate retention periods for records required by law or necessary for legal claim or regulatory compliance purposes. For example, asbestos records may be required as evidence or for defending potential claims which may only appear for up to 40 years after initial exposure.

The policy sets out a number of category-specific retention schedules with recommended periods for different record types for categories such as:

- accounting and tax
- Companies Act
- employment and pensions
- information management
- insurance
- intellectual property
- pre-qualifications
- tenders and contracts
- property
- quality assurance
- safety, health and environmental records
- shares and dividend records

The policy also built in key principles for working out appropriate retention periods outside the categories. For instance, these included the need to:

- account for GDPR and data protection law requirements to only keep personal data as long as necessary;
- maintain legal hold on data or records relevant to legal or regulatory proceedings;
- hold records for the longer recommended period where a record is in more than one category;
- make sure the retention period is proportionate to the length of time for which the record may still be useful; and
- consider whether the record may be required for regulatory compliance, evidence or audit purposes and whether there is a legitimate business need to keep it.

It was important to emphasise in the policy that all employees, whether permanent, temporary, agency staff or contractors, were responsible for effectively managing the business's paper and electronic records in line with the policy principles. And that the policy should be read alongside other applicable policies, such as our data protection policy.

Managing and maintaining an effective records management policy and culture is an ongoing journey and iterative process. It requires consistent training and targeted communications as well as a willingness to regularly review and adapt policies in practice so they can change over time while accommodating new retention requirements and business needs as technology changes.

In terms of challenges, we often found our records management policy was difficult for staff to understand and / or apply in practice when archiving documents. We therefore included retention as part of our mandatory data protection e-learning module and set up a working group with stakeholders from our Property team, who manage physical archiving, to help make sure our retention policies line up with our physical archiving processes.

We continue to work closely with our IT function on new technology so staff are better able to apply retention periods to electronic data whether on email or databases. We have set up a working group to review broader data governance issues and retention is a key workstream. Our Operational Audit function also support by carrying out audits on project teams which include how business units manage retention at project level.

Acknowledgements

The DPN Data Retention Working Group, which developed and wrote this guidance was chaired by Robert Bond (Bristows LLP) and among others included:

Dominic Batchelor (Royal Mail), Stephen Baigrie, Sarah Blacker (Royal Mail), Simon Blanchard (DPN Associates), Michael Bond (NewsUK), Emma Butler (Yoti), Gerald Coppin, Liz Curry (Liz Curry & Co), John W Cush, Marc Dautlich (Bristows LLP), Paul Dawson-Hart (Member360), Philippa Donn (DPN Associates), Tim Drye (DataTalk), Fedelma Good (PwC UK), Sara Howers, Matthew Kay (Thomson Reuters), Martine King (Barnardo's), Sayid Madar, Michele Masnaghetti (Epsilon Abacus), David Morgan (OneSavings Bank plc), Neil Paterson (TUI Group), Janine Regan (Norton Rose Fulbright LLP), Claire Robson, Noga Rosenthal (Ampersand), Pheobe Rowson-Stevens (Thomson Reuters), Daniel Sullivan and Beth Whitehand.

DATA PROTECTION NETWORK

The Data Protection Network (DPN) publishes expert analysis, insight and resources. Our content is written and developed by a team of data protection specialists, members of our Advisory Board and other respected contributors. In 2017 the DPN published the first definitive industry guidance on legitimate interests.

The DPN is run by DPN Associates Ltd, a data protection consultancy which provides accessible practical privacy advice to businesses across a range of sectors. Based on extensive real-world experience, our team continues to stay at the forefront of data protection.

To learn more about us visit:
https://dpnetwork.org.uk

Bristows

We are Bristows, the world's specialist law firm for clients that innovate. We help clients grow in life sciences, technology and other dynamic sectors. Clients on the edge of tomorrow; those creating new technologies and ideas, and those embracing them.

With one of the biggest and most well-known teams in Europe, Bristows is the go-to firm for pragmatic, expert-informed data protection advice. Our clients rely on us for guidance on a huge range of data protection issues, with our recommendations always rooted in pragmatism and what will actually work for their business.

To learn more about us visit:
https://www.bristows.com

exterro®

About Exterro

Exterro®, Inc. is the leading provider of privacy, e-discovery and information governance software specifically designed for in-house legal, privacy and IT teams at Global 2000 and Am Law 200 organisations.

Exterro was founded with the simple vision that applying the concepts of process optimisation and data science to how companies manage digital information and respond to litigation would drive more successful outcomes at a lower cost. We remain committed to this vision today, as we deliver a fully integrated Legal GRC platform that enables our clients to address their regulatory, compliance and litigation risks more effectively and at lower costs.

Trusted by the Association of Corporate Counsel and installed as the ACC's exclusive Alliance Partner for data privacy, compliance, and e-discovery, Exterro's software solutions span privacy, legal operations, compliance, cybersecurity and information governance, helping the world's largest organisations work smarter and more efficiently.

Data Privacy

Exterro's Privacy solutions enable your team to quickly and easily orchestrate processes for complying with critical requirements of the GDPR, CCPA and other privacy regulations. With the Exterro Suite, your teams can quickly and defensibly develop and maintain a data inventory, respond to data subject access requests, conduct 3rd party risk profiles, implement automated policies that will find PII across your IT infrastructure and enforce business rules for storage, retention and protection of personal data.

E-Discovery

Exterro's software platform unifies the entire e-discovery process, enabling users to get to the facts of the case sooner at a fraction of the cost. It is available as a complete end-to-end solution or as individual products.

The Exterro Platform is a single, natively built, fully integrated solution that unifies all of Exterro's E-Discovery and Information Governance products. Further, it includes our *integration hub*, which connects to the industry's broadest range of 3rd party tools, system applications, and data sources, orchestrating processes across applications and minimising your cost of ownership.

To learn more about Exterro and schedule a software demonstration, visit: *https://www.exterro.com/*

Appendix A – Considerations and sample templates for specific data types

Company records

All companies in the UK registered under the Companies Act 2006 (CA 2006) have to create and maintain certain company records, including registers, accounting records, minutes, memorandums and agreements. There will be similar requirements in different territories.

Company records may contain personal data such as names and addresses, and in some cases other personal data such as dates of birth. Therefore, data protection laws are relevant for a retention policy to make sure personal data in such records is processed lawfully.

The CA 2006 sets mandatory retention periods for certain company records. Keeping these records in line with the requirements will be 'lawful processing' for GDPR purposes because the retention is necessary to comply with a legal obligation on the company (as the controller). *(See GDPR 6(1)(c))*.

If a company wishes to keep a record containing personal data for longer than required by CA 2006, they will need to consider whether a longer period is justifiable when they balance data protection considerations against the company's other interests. Or in cases where the CA 2006 is silent, what period is appropriate in the circumstances.

A typical justification for a retention period longer than one set by CA 2006 is the relevant statutory limitation period for actions against the company after the CA 2006 retention period has passed. *(See Directors Service Contracts below)*.

Or, it may be necessary to keep certain records for tax purposes (see Directors Service Contracts below) or to show compliance with other legal obligations *(See Certificate of Incorporation below)*.

The table below sets out the statutory retention period for a select list of company records that are likely to contain personal data. This guidance cannot provide a detailed review of the law relating to retention of company records but there is more information in the ICSA Guide to Document Retention[9].'

9 A.C. Hamer (2011), The ICSA Guide to Document Retention, 3rd Edition, ICSA Publishing Limited, Chapter 12.

Please note this template is an example. Retention periods need to be internally agreed and justified.

Company records

Category of data	Paper or electronic	Retention period
Register of members	Both	You can remove entries added on or after 6 April 2008 from the register 10 years after the person stops being a member (section 121 CA 2006). You must keep entries made before 6 April 2008 for 20 years after the person stops being a member (schedule 4, paragraph 2 Fifth CA 2006 Commencement Order).
Register of directors' residential addresses	Both	You must keep this register for the life of the company (Section 162 CA 2006) and there is no provision to remove entries of former directors. Note: you cannot make this register available for public inspection.
Directors' service contracts	Both	You must keep a copy of the contract or a memorandum of its terms for at least one year from the expiry or termination date (Section 228 CA 2006). However, it is advisable to keep the contract for up to six years following expiry for tax purposes and to account for the 6-year limitation period for contracts.
Board minutes	Both	For board meetings held on or after the 1 October 2007, you should keep copies of the minutes for 10 years from the date of the meeting (section 248 CA 2006). If the minutes contain personal data, you should not keep them for longer than the set 10-year period unless they are still 'necessary' for the purposes for which the data is processed. For meetings held before 1 October 2007 you should keep the minutes permanently (section 382 Companies Act 1985).
Certificate of Incorporation and Memorandum of Association	Both	There is no legal requirement to keep the Certificate of Incorporation or the Memorandum of Association. However, as these documents evidence the company's compliance with the registration requirements of the CA 2006 (section 15 CA 2006), it may be wise to keep the original documents for the life of the company.

Continued

Company records	
Authority:	[Compliance Team]
Information asset owner:	[Company Secretary]
Location held:	[To be specified] Example: At the company's registered office or SAIL (single alternative inspection location). However, the certificate of incorporation / memorandum of association and the register of directors' residential addresses may be held elsewhere as there is no legal requirement to keep in a specific place.
Permanent preservation:	Only required for the register of directors and board minutes of meetings held before 1 October 2007.
Statutes that apply:	Companies Act 2006, Companies Act 1985
Special categories of data:	No

Employee records

Employee data processing will be for multiple purposes, mainly to:

- comply with employment contract obligations;
- satisfy legal obligations; and
- provide other employee services and benefits.

There are statutory data retention periods that affect certain employment data (such as payroll and pensions). The Chartered Institute of Payroll Professionals (CIPP) recommends certain non-statutory periods for other types of UK employment processing.

Different retention rules are likely to apply in different countries. It's therefore important to consider local law requirements where necessary. Human resources information systems should also have automatic deletion / archiving periods to reflect the agreed retention periods.

The HR (or other responsible team / person) should review the example retention schedule set out below against any retention periods applied by individual functions. You might wish to add the location of the data too. You should inform individuals of retention periods, such as in an applicant privacy notice and employee privacy notice).

Please note this template is an example. Retention periods need to be internally agreed and justified.

Employment data		
Category of data:	Paper or electronic:	Retention period:
Job application, CVs and interview notes and references of successful job candidates	Both	Length of employment plus 6 years.
Job application, CVs and notes of unsuccessful job candidates	Both	Typically, 6-12 months.
Criminal Background Checks (CBC) (where you are allowed to collect this data)	Both	For successful candidates: the retention period should match other employment records. Checks on unsuccessful candidates: approximately 6 to 18 months. This will depend on the context.
Records relating to sick leave and absence	Both	Length of employment plus 6 years.
Performance appraisals and disciplinary records	Both	Length of employment plus 6 years.
Training records	Both	Length of employment plus 6 years.

Continued

Employment data		
Category of data:	Paper or electronic:	Retention period:
Working time records (overtime, annual holiday, jury service, time off for dependents, and so on)	Both	2 years.
Essential medical data required for employment purposes	Both	Length of employment plus 6 years.
Occupational health data and referrals	Both	Length of employment plus 6 years.
Benefits records	Both	Length of employment plus 6 years.
Payroll records (including Statutory Sick Pay, National Minimum Wage, salary sacrifice)	Both	Length of employment plus 6 years. *Also see Finance Records.*
Maternity and paternity records	Both	5 years from birth or adoption
Pensions records	Both	12 years from the end of any payable benefit.
Health and safety records (including accidents at work)	Both	*See Health and Safety and Environmental Records*
Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH) and Control of Asbestos at Work	Both	40 years from the date of the last entry for most hazardous substances including asbestos. 75 years for exposure to radiation. *Also see Health and Safety and Environmental Records*
TUPE records (for employees who have transferred employer)	Both	Length of employment plus 6 years.
Trades Union or collective agreements (such as pay)	Both	6 years after the agreement ends.

Continued

Employment data	
Authority:	[To be specified]
Information asset owner:	[Head of HR]
Location held:	[HR systems]
Permanent preservation:	No
Statutes that apply (UK):	Employment Rights Act 1996. Working Time Regulations 1998. Age Discrimination in Employment Act (ADEA).
Special categories of data:	Yes, where necessary, including essential medical data, data to comply with anti-discrimination law, trades union membership and evidence of consent (where required) for such processing.

Health and safety and environmental records

You should make sure you have a retention policy for health and safety and environmental data. The table below sets out a non-exhaustive example of a retention schedule with guide retention periods for typical data categories for health and safety and environmental data.

You would need to review this with your organisation's health and safety, legal, data protection, environmental and sustainability compliance teams, and tailor it so it covers any specific retention issues or local law requirements relevant to your business.

The table below takes account of any minimum UK statutory retention requirements or periods for potential legal or regulatory proceedings This is to the extent that the data categories below contain 'personal data'. Organisations will also need to justify that retention of personal data is necessary and for legitimate purposes.

Please note this template is an example. Retention periods need to be internally agreed and justified.

Health and safety and environmental records		
Category of data:	Paper or electronic:	Retention period:
Health and safety policies, systems, procedures, standards and guidance.	Both	Life of Group entity* As required for evidence of compliance. Health and Safety at Work Act 1974 (as amended).
Health and safety documents and records (including Annual summary, audit reports, incident notifications, investigation reports, safety alerts, training records, risk assessments carried out in compliance with law and method statements, correspondence with regulators, advice and related safety record correspondence).	Both	Life of Group entity* Evidence of compliance with statutory provisions in UK or overseas legislation where appropriate. Management of Health and Safety at Work Regulations 1999.

Continued

Health and safety and environmental records		
Category of data:	Paper or electronic:	Retention period:
Incident, disease and dangerous occurrence books (such as 'accident books') and records including electronic records for reported accidents and incidents.	Both	Minimum of 3 years from date of last entry or 7 years from reporting. Or, if accident involves a child / young adult, then until that person reaches 21. Evidence of compliance with UK Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 or local or overseas legislation where appropriate.
Environmental records and assessments (including electronic records and database entries)	Both	Life of Group entity* Evidence of compliance with statutory provisions in UK or overseas legislation where appropriate.
Medical and occupational health records (including medical assessments prior to or during employment) Note: this is special category of data under the Data Protection Act 2018 and GDPR.	Both	Minimum of 40 years from date of last entry for UK except for records of exposure to asbestos, lead and / or ionizing radiation which have specific statutory rules as below. Evidence of compliance with statutory provisions in UK or overseas legislation where appropriate. If the business closes, it has to provide records to local HSE office in UK (COSHH Regs, ACOP para 253).
Medical and occupational health records and medical examination certificates concerning exposure to asbestos	Both	Records: Date of last entry plus 40 years. Certificates: Date of issue plus 4 years. The Control of Asbestos at Work Regulations 2002. Control of Asbestos Regulations 2006. Control of Asbestos Regulations 2012.
Medical records and details concerning exposure to lead	Both	Date of last entry plus 40 years. The Control of Lead at Work Regulations 1998 as amended by the Control of Lead at Work Regulations 2002.

Continued

Health and safety and environmental records		
Category of data:	Paper or electronic:	Retention period:
Medical records concerning exposure to ionizing radiation	Both	Until the person reaches 75, but in any event for at least 30 years from the date of the last entry. The Ionising Radiations Regulations 2017.
Medical examinations at work related to hazardous substances (ensuring maintenance of employee health record)	Both	Minimum of 40 years from date of last entry made for UK where record representative of personal exposures of identifiable employees or in any other cases, at least 5 years, from last entry made. Regulation 10(5), Control of Substances Hazardous to Health Regulations 2002, SI 2002/2677.
Records of tests and examinations of control systems and protective equipment concerning exposure to other substances hazardous to health	Both	Date tests were carried out plus 5 years. The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH).
Register of employees who work in dangerous conditions or whose health is otherwise at threat regarding exposure to substances hazardous to health	Both	Minimum 5 years. However, where record is not representative of personal exposures of identifiable employees, 40 years from date of last register entry. Regulation 10(5), Control of Substances Hazardous to Health Regulations 2002, SI 2002/2677.
Register of employees who work with 3rd and / or 4th category biological agents	Both	40 years from date of last register entry. Schedule 3, paragraph 4, Control of Substances Hazardous to Health Regulations 2002, SI 2002/2677.
Register of employees exposed to airborne asbestos (including employee health records)	Both	40 years from date of last register entry. Regulation 22(1) Control of Asbestos Regulations 2012, SI 2012/632.
Register of work and rest periods and working time opt-out forms	Both	Minimum of 2 years. Regulations 5 and 9 Working Time Regulations 1998 (SI 1998/1833).

Continued

Health and safety and environmental records		
Category of data:	Paper or electronic:	Retention period:
Data re emergency medical care, individual reintegration plans, workplace adjustments, individual treatment agreements, fitness for work	Both	Maximum of 6 years after expiry of employment. Limitation Act 1980, Data Protection Act 2018 and GDPR
Records and minutes of consultations with safety representatives and committees	Both	Minimum of 10 years Evidence of compliance with Safety Representative and Safety Committees Regulations 1977 and Safety (Consultation with Employees) Regulations 1996.
Fire risk assessment	Both	Date of last fire risk assessment plus 5 years. Evidence of compliance with the Regulatory Reform (Fire Safety) Order 2005.
Environmental data regarding dangerous chemicals, substances, or measures re these for manufacturing / import or distribution of products	Both	Minimum 10 years. Article 49 Regulation 1272/2008/EC Article 36 of the Regulation 1907/2006/EC (REACH).
Names and addresses of customers / buyers of environmentally dangerous substances or measures	Both	Minimum 10 years. Article 49 Regulation No 1272/2008/EC on classification, labelling and packaging of substances and mixtures.
Environmental permit documentation	Both	Specific periods will apply and vary, depending on the nature of the permit. In general, you should keep permits for as long as they remain valid, and thereafter as necessary for evidence purposes in any potential regulatory or third-party claim, litigation or liability.

Continued

Health and safety and environmental records		
Category of data:	Paper or electronic:	Retention period:
Manufacturer documents re conformity assessment / statement of an energy-consuming product	Both	Minimum 10 years. Regulation 9, Eco-design for Energy-Related Products Regulations 2010/2617.
Technical specification documentation and performance declarations on construction products	Both	Minimum 10 years. Article 11 Regulation (EU) No 305/2011, laying down harmonised conditions for the marketing of construction products and repealing Council Directive 89/106/E.
Copy of documents re transfer of waste materials by competent authority	Both	Minimum 3 years from transfer. Article 20 of the Regulation (EC) No 1013/2006 on Shipments of Waste.
Data on nature, quality and composition of waste re obligations of producer, holder or consignor of hazardous waste to retain records	Both	Minimum: length of time as holder of the waste and a further 3 years. Regulation 49(3) Hazardous Waste (England and Wales) Regulations 2005 (as amended).
Technical documentation on noise emissions	Both	Minimum 10 years. Regulation 7, Noise Emission in the Environment by Equipment for use Outdoors Regulations 2001/1701. Directive 2000/14 of the European Parliament and of the Council of 8 May 2000 on approximation of the laws of the Member States relating to the noise emission in the environment by equipment for use outdoors and EC-statement.

Continued

Health and safety and environmental records	
Authority:	[Health and Safety and / or Sustainability or Environmental compliance function]
Information asset owner:	[Health and Safety or Sustainability or Environmental compliance Director]
Location held:	[To be specified]
Permanent preservation:	Where specified – *however, to the extent that the data is 'personal data' GDPR and / or the Data Protection Act 2018 will still apply where relevant, and organisations will still need to justify that retention is necessary.
Statutes that apply:	[To be specified]
Special categories of data:	Where specified

Children's records

The GDPR identifies children as needing 'specific protection' because they are less aware of the risks, consequences and safeguards involved in processing their personal data.

So, while children have the same rights as adults over their personal data, there are some child-specific provisions. However, none of these refer specifically to how long to keep children's data, just that their data should have extra protection.

GDPR allows member state derogations on the definition of a child. The UK's 2018 Data Protection Act says a child is an under 18 for safeguarding purposes (which includes health and social care records), but, for example, 13 for online services.

A child in England, Wales or Northern Ireland can make their own rights request 'as long as they are competent'. However, in Scotland, those 12 or over are considered to be mature enough.

The first decision an organisation needs to make is at what age a person moves from being a child to an adult. This decision will usually depend on:

- the nature of the business;
- the processing purpose;
- any sector-specific laws; and
- where in the UK the data is created, as there can be regional differences.

The age identified could be as low as 12 and as high as 18.

The organisation then needs to determine if this has an impact on the length of time they should keep the data.

There is no statutory limit for keeping children's data for marketing or fundraising purposes, although there are standards on fundraising involving children which set age limits (either as a fundraiser or a donor) which may help inform your decision-making process. Therefore, for these record types you may decide to follow the guidelines you have set for adults. (See *Marketing records* for examples of what to consider here.)

Organisations providing social and / or healthcare services to children are governed by various regulations that define specific retention periods depending on the nature of that care.

It is important for organisations who work with children receiving health and social care services to develop clear guidelines for keeping, storing and getting rid of records. A retention schedule is a necessary part of developing a safeguarding policy and procedures as well as for GDPR compliance.

Below is an example retention schedule from a children's charity. Note that there are different retention periods for different countries.

Please note this template is an example. Retention periods need to be internally agreed and justified

Children's data

Category of data – service users	Paper or electronic	Retention period
Safeguarding: child sexual exploitation, trafficking, sexually harmful behaviour, serious case reviews	Both	100 years
Domiciliary day care, children's centres, respite day care, early years services, childminding, Sure Start and play group case records (England, Scotland and Wales)	Both	6 years
Domiciliary day care, children's centres, respite day care, early years services, child minding, Sure Start and play group case records (Northern Ireland)	Both	8 years
Children's records where there is no statutory retention period	Both	6 years
Looked After Children (LAC): leaving care	Both	75 years
LAC: overnight domiciliary care (England, Northern Ireland and Wales)	Both	75 years
LAC: overnight domiciliary care (Scotland)	Both	100 years
LAC: residential children's homes and schools (England, Northern Ireland and Wales)	Both	75 years
LAC: residential children's homes and schools (Scotland)	Both	100 years
LAC: supported lodgings	Both	75 years
Children's rights case file (Scotland)	Both	100 years
Family placement: adoption post-2006	Both	100 years
Family placement: adoption pre-2006	Both	75 years
Post-adoption access to records and tracing, historic abuse, disclosures to external authorities, birth relative support for tracing adopted children	Both	100 years
Indirect services	Both	Until 18th birthday
Family placement: adoption referrals with no further action (Northern Ireland)	Both	Up to 18th birthday of child
Family placement: fostering (England, Northern Ireland and Wales)	Both	75 years
Family placement: fostering (Scotland)	Both	100 years
Residential Special School records day care	Both	25 years
Post-care subject access requests, historic abuse enquiries, disclosure inquiries to external authorities (self)	Both	75 years

Category of data - employees

Category of data – service users	Paper or electronic	Retention period
Children's Services employee: job history	Both	75 years
Children's Services: training records	Both	75 years
Children's Services: appraisals	Both	75 years
Children's Services: disciplinary matters	Both	75 years

Category of data – carers

Category of data – service users	Paper or electronic	Retention period
Family Placement: adoption	Both	75 years
Family Placement: fostering - potential carers initial enquiry only	Both	1 year
Family Placement: fostering - potential carers initial visit only	Both	3 years
Family Placement: fostering - potential carers with safeguarding concerns	Both	75 years
Family Placement: fostering and adoption - applicant refused, not approved or withdrawn (England, Northern Ireland and Wales)	Both	6 years
Family Placement: fostering and adoption - applicant refused, not approved or withdrawn (Scotland)	Both	25 years
LAC: supported lodgings	Both	15 years
Family Placement: fostering (England, Northern Ireland and Wales)	Both	75 years
Family Placement: fostering (Scotland)	Both	100 years
Authority:	[To be specified]	
Information asset owner:	[To be specified]	
Location held:	[To be specified]	
Statutes that apply:	[To be specified]	
Special categories of data:	[Where specified]	

Medical records

Records of NHS organisations are public records under Schedule 1 of the Public Records Act 1958. Public health and social care records, where a local authority is the provider, must be managed in line with the requirement to make proper arrangements under Section 224 of the Local Government Act 1972.

For staff working in health and social care, there are a number of record-keeping codes that people associated with certain professional bodies must comply with as part of their profession. Your records manager should review these example retention periods against any retention periods from the Department of Health or other relevant regulatory body.

Please note this template is an example. Retention periods need to be internally agreed and justified

Medical records

Category of data	Paper or electronic	Retention period
General Practitioner records	Both	Life of the patient plus at least 10 years after death.
General adult health records (Ensure reference to NHS Codes of Practice)	Both	8 years from discharge or when patient last seen.
Mental health records	Both	20 years from discharge or when patient last seen or 8 years after the patient has died.
Cancer / oncology records	Both	30 years from diagnosis of cancer or 8 years after the patient has died.
Children's records including midwifery, health visiting and school nursing	Both	Until the patient's 25th birthday or, if the patient was 17 at the end of treatment, until their 26th birthday.
Clinical trials master file	Both	30 years after trial ends.
Authority:	[To be specified]	
Information asset owner:	[To be specified]	
Location held:	[To be specified]	
Permanent preservation:	No	
Statutes that apply:	Records Management Code of Practice for Health and Social Care 2016.	
Special categories of data:	Yes	

Clinical trial records

Organisations have a statutory duty to make arrangements to keep and / or get rid of clinical trial records. This covers documents received or created and all records and documents regardless of form (electronic or paper records). You need to comply with legal, regulatory, quality and corporate requirements.

Please note this template is an example. Retention periods need to be internally agreed and justified

Clinical trial records

Department	Category of data	Paper or electronic	Retention period
Business development	Proposals, presentations communications relating to a project	Both	Review status of project documents annually to determine if the retention period has passed, or the project status has changed.
	Department / internal communication	Both	If no deal, then destroy 4 years after the creation date. If collaboration goes ahead, then keep for lifetime of deal.
Clinical	Trial Master File	Both	Review status of project documents annually to determine if the retention period has passed, or the project status has changed.
	Pre-clinical material	Both	Maintain reports. Other material such as Wet Tissue may be destroyed 15 years after study ends.
	Department / internal communication	Both	4 years after creation date.
	Radiation protection and x-ray regulation documents	Both	30 years after end date of the work involving exposure.
Development	Project documents	Both	Review status of project documents annually to determine if the retention period has passed, or the project status has changed.
	Department / internal communication	Both	4 years after creation date.
	Non-GLP test records, test records not required for product certification	Both	2 years after creation date.

Continued

Clinical trial records

Department	Category of data	Paper or electronic	Retention period
Production	Project documents (design)	Both	Review status of project documents annually to determine if the retention period has passed, or the project status has changed.
	Project documents (non-design)	Both	4 years after creation date.
	Department / internal communication	Both	4 years after creation date.
	Product records, non-implantable	Both	5 years after date of last product manufacturing.
	Product records, implantable	Both	15 years after date of last product manufacturing.
Facilities	Various Facilities documents (such as lease)	Both	Range of retention periods depending on document type.
Financial	Financial records	Both	Later of statutory financial retention requirements, or end of commercialisation for a project.
	Department / internal communication	Both	4 years after creation date.
Health and Safety	Occupational investigations	Both	10 years after investigation date.
	Other H and S documents	Both	Range of retention times depending on document type.
Human Resources	Applications for Jobs – unsuccessful	Both	6 months
	Employee records	Both	7 years after end date.
	Pension information	Both	12 years
	Department / internal communication	Both	12 years
Information Technology	Department documents	Both	4 years after creation date.
	Back up tapes	Both	3 months
Intellectual Property	Various IP documents	Both	Range of retention times depending on document type.

Continued

Clinical trial records			
Department	Category of data	Paper or electronic	Retention period
Legal	CDAs, contracts and agreements	Both	7 years after the agreement expiry.
	Patents, trademarks	Both	12 years after registration expires.
	Litigation files	Both	20 years after litigation closes.
	Opinion letters / memos	Both	20 years after creation.
	Department / internal communication	Both	4 years after creation date.
Quality	eDMS documents	Both	10 years after the manufacture of the last product to which documents relate.
	Training records	Both	20 years
	Quality documents	Both	10 years after creation date.
	Department /internal communication	Both	4 years after creation date.
	Notified body documents and correspondence	Both	10 years after manufacture of last product to which the document(s) relate.
Regulatory	Trial Master File and pre-clinical material	Both	Review status of project documents annually to determine if the retention period has passed, or the project status has changed.
	Correspondence with HAs (questions, responses, cover letters, DSURs, meeting minutes, approvals, scientific advice, orphan drug applications, annual reports and so on)	Both	Review status of project documents annually to determine if the retention period has passed, or the project status has changed.
	Device regulatory documents	Both	Review status of project documents annually to determine if the retention period has passed, or the project status has changed.
	Department / internal communication	Both	4 years after creation date.
	RoHS documents (2011/65/EU)	Both	10 years after the electrical and electronic equipment has been placed on the market.

Continued

Clinical trial records			
Department	Category of data	Paper or electronic	Retention period
Regulatory	Anti-money laundering regulations	Both	5 years from record creation.
Respiratory Development	Project documents	Both	Review status of project documents annually to determine if the retention period has passed, or the project status has changed.
	Department / internal communication	Both	4 years after creation date.
Secretariat	All documentation	Both	Indefinitely
Authority:		[To be specified]	
Information asset owner:		[To be specified]	
Location held:		[To be specified]	

References

Articles of Association (Secretariat records).

Companies Act 2006 (Financial records).

Dir 93/42, Annex II, 6.1 (Medical device records).

HMRC (Financial records).

HSE (H & S records).

ISO13485 (Medical Device records).

ICH E6 (GCP records).

GMP (Product Development records).

The UK Good Laboratory Practice Regulations (Statutory Instrument 1999 No, 3106, as amended by Statutory Instrument 2001 No.994).

OECD Principles of Good Laboratory Practice (as revised in 1997), ENV/MC/CHEM (98) 17.

EU General Data Protection Regulation (2016/679).

Data Protection Act 2018.

Limitation Act 1980.

Anti-money laundering regulations.

Finance, accounting and tax records

Storing financial data in the context of data protection can be tricky, given the potential sensitivities of data dealing with money. Some of the requirements for keeping financial data come from the need to hold evidence for statutory and regulatory purposes. However, data protection considerations also apply where the data is personal data.

For example, information referring to directors and officers, their pay and registered addresses. Other information may be necessary as evidence of personal transactions, for example, expenses paid through corporate bank accounts, with individuals' names used as a reference, so they can be matched against receipts for accounting reconciliation purposes.

This may include cheque stubs (where records exist), individual tax returns and tax appeals, or other personalised records. For payroll and bonus computations, it may be necessary to identify individuals who will receive a certain level of bonus or additional pay such as individual commission or other performance-related pay.

The finance function should regularly review these example retention periods against any retention periods or practices from the business and associated functions. Finance data will be held or evidenced in accounting, tax and transactional records.

Table A: General accounting and finance records

Please note this template is an example. Retention periods need to be internally agreed and justified

General accounting and finance records		
Category of data	Paper or electronic	Retention period
Financial (including audit) – statutory reporting	Both	7 years from financial year end (statutory limitation period).
Financial (including audit) – management accounting	Both	7 years from financial year end (statutory limitation period).
Financial (including audit) – sales and purchases	Both	7 years from financial year end (statutory limitation period).
Financial (including audit) – import / export	Both	7 years from financial year end (statutory limitation period).
Financial (including audit) – cash / banking records	Both	7 years from financial year end (statutory limitation period).
Financial (including audit) - tax	Both	10 years from tax year end or as required in a tax investigation.
Financial (including audit) - audit	Both	10 years from financial year end or as required to support risk registers.

Continued

General accounting and finance records	
Authority:	Finance Team
Information asset owners:	Chief Financial Officer, Senior Accounting Officer
Permanent preservation:	You may need to keep records of fraud and criminal investigations for longer than 10 years. You must hold summary records which evidence an individual's net, tax and gross transaction amount as a statutory record, but details of each transactional item which makes up the net total is not required.
Statutes that apply:	Companies Act 1985 as amended by the Companies Acts 1989 & 2006.
Special categories of data:	Yes*

*The organisation's finance team should review this. While it may be unlikely that the financial categories listed would contain data granular enough to be special category data, we acknowledge that this may depend on an organisation's systems. For example, there could be expense entries which contain references to illness / health data.

Table B: Specific accounting, tax and finance records

Please note this template is an example. Retention periods need to be internally agreed and justified

Specific accounting, tax and finance records			
Category of data	Paper or electronic	Retention period	Legal reference
Accounting records (including; bank statements and reconciliations; payment and receipt records; supplier / accounts payable invoices; customer / accounts receivable invoices; customer debit notes; purchase and sales ledger; employee expense records)	Both	3 years from financial year end for private companies 7 years from financial year end for public limited companies Complete audit should be held for 10 years or as required for risk register purposes, or to the end of any tax enquiry, if longer.	Companies Act 1985 as amended by the Companies Acts 1989 & 2006. Generally Accepted Accounting Practice (UK GAAP).

Continued

Specific accounting, tax and finance records			
Category of data	Paper or electronic	Retention period	Legal reference
Accounting record (including audit): taxation	Both	10 years from tax year end or as required in the event of a tax investigation.	As above
Annual audited financial statements and report	Both	Life of Group entity	As above
Interim financial statements	Both	Life of Group entity	As above
Internal financial statements	Both	7 years from financial year end	As above
Annual plans and budgets	Both	7 years from financial year end	As above
VAT records	Both	7 years from tax year end	Value Added Tax Act 1994 (as amended).
Dividend withholding tax	Both	7 years from tax year end	Section 1104 of Corporation Tax Act 2010.
Corporation tax self-assessment records	Both	7 years from tax year end	Taxes Management Act 1970.
Stamp duty land tax records	Both	7 years from tax year end	Paragraph 9, Schedule 10, Finance Act 2003 (as amended).
Landfill tax records	Both	7 years from tax year end	The Landfill Tax Regulations 1996 (as amended).
Insurance premium tax records	Both	7 years from tax year end	The Insurance Premium Tax Regulations 1994.

Continued

Specific accounting, tax and finance records			
Category of data	Paper or electronic	Retention period	Legal reference
Charitable donation records	Originals	Records re sponsorship arrangements or partnerships with third party charities: 6 years after date of last payment but up to 12 years if any payments are still outstanding or there is disputes regarding a document executed as a deed Documents evidencing donations made to charitable organisations: public companies: 6 years private companies: 3 years	Section 388(4) Companies Act 2006.
Banking records:			
Cheques and other negotiable instruments	Originals	6 years from date of issuance	
Paying-in counterfoil	Originals	6 years from date of issuance	
Bank statements and reconciliations	Original if provided in hardcopy or otherwise if statements obtained via internet banking, on-line printouts	Public Companies: 6 years / Private Companies: 3 years	
Instructions to bank	Both	6 years after ceasing to be effective	

Continued

Specific accounting, tax and finance records	
Authority:	Finance Team
Information asset owner:	Chief Financial Officer, Senior Accounting Officer
Permanent preservation:	You may need to keep records of fraud and criminal investigations for longer than 10 years. Summary records which evidence an individual's net, tax and gross transaction amount must be held as statutory record, but details of each transactional item which makes up the net total is not required.
Statues that apply:	See legal references above.
Special categories of data:	Yes*

*The organisation's finance team should reviewed this.

Table C: Contracts and procurement records

Please note this template is an example. Retention periods need to be internally agreed and justified

Contracts and procurement records			
Category of data	Paper or electronic	Retention period	Legal reference
Contracts (under hand) and relevant correspondence and other related documents (such as PO, credit checks)	Both	End of contract plus 7 years (or to the end of any warranty or service periods, if longer)	Limitation Act 1980.
Contracts (executed as a deed) and relevant correspondence and other related documents (such as PO, credit checks)	Both	End of contract plus 13 years (or to the end of any warranty or service periods, if longer)	Limitation Act 1980.
Tenders / bids for contracts made by Group / Entity (unsuccessful)	Both	Last correspondence plus 2 years	

Continued

Contracts and procurement records			
Category of data	Paper or electronic	Retention period	Legal reference
Tenders / bids for contracts made by Group / Entity (successful)	Both	End of contract plus 7 years (or to the end of any warranty or service periods, if longer)	Limitation Act 1980.
Tenders / quotes from suppliers (unsuccessful)	Both	Last correspondence plus 2 years	Limitation Act 1980.
Tenders / quotes from suppliers (successful)	Both	End of contract plus 7 years (or to the end of any warranty or service periods, if longer)	Limitation Act 1980.
Authority:	Finance Team		
Information asset owner:	Chief Financial Officer, Senior Accounting Officer		
Permanent preservation:	You may need to keep records of fraud and criminal investigations for longer than 10 years. Summary records which evidence an individual's net, tax and gross transaction amount must be held as statutory record, but details of each transactional item which makes up the net total is not required.		
Statutes that apply:	See legal references above.		
Special categories of data:	Yes*		

*The organisation's finance team should review this.

Table D: Payroll records

Please note this template is an example. Retention periods need to be internally agreed and justified

Payroll records			
Category of data	Paper or electronic	Retention period	Legal reference
Income tax records and returns for NI and other deductions from employees' salaries, income tax records and correspondence with relevant authority	Both	7 years (or to the end of any tax enquiry, if longer)	The Income Tax (Employments) Regulations 1993 as amended.
PAYE records (post April-2004) which are not required to be sent to HMRC	Both	Not less than 3 years after the end of the tax year to which the records relate	Income Tax (PAYE) Regulations 2003, Reg. 97.
Minimum wage records	Both	End of the pay reference period following the one that the records cover plus 3 years	National Minimum Wage Act 1998.
Records concerning parental leave / maternity pay or equivalent	Both	End of the tax year in which the parental leave / maternity period ends plus 3 years	The Statutory Maternity Pay (General) Regulations 1986 as amended.
Records concerning pay due to employees during absence from work due to illness	Both	End of the tax year to which they relate plus 3 years	The Statutory Sick Pay (General) Regulations 1982 as amended.
Working time records	Both	Date on which they were made plus 2 years	The Working Time Regulations 1998.

Continued

Payroll records	
Authority:	Finance Team
Information assets owner:	Chief Financial Officer, Senior Accounting Officer
Permanent preservation:	You may need to keep records of fraud and criminal investigations for longer than 10 years. Summary records which evidence an individual's net, tax and gross transaction amount must be held as statutory record, but details of each transactional item which makes up the net total is not required.
Statutes that apply:	See legal references above.
Special categories of data:	Yes*

*The organisation's finance team should reviewed this.

Insurance records

'Insurance records' covers a potentially very broad class of records. This guidance cannot provide details of all the types and typical content of insurance records and the many parties involved in creating, maintaining and / or sharing these records.

There are a limited number of mandatory rules in the UK about keeping 'insurance records.' A broad overview of these records is a starting point for a retention policy for them.

Insurance records are generated at every stage in the lifecycle of virtually all types of insurance product[10]. Insurance records differ greatly in nature and content depending on the stage at which they are generated in the lifecycle of the insurance in question.

The main lifecycle stages depend on the type of insurance. However, as a very general rule, these stages typically include marketing, underwriting, administering and reinsuring, as well as claims handling, including legal proceedings.

Each of these stages creates different 'insurance records'. These records include:

- the insurance contract itself.
- information provided by policyholders or their agents in proposal forms.
- fraud checks carried out by or on behalf of the insurer (both at underwriting and in claims).
- documents to support claims (such as medical records, police reports and so on).

Typically, the parties involved include:

- brokers (both in respect of insurance and reinsurance);
- insurers or coverholders (who may be formed as a syndicate, for example, the London Lloyds insurance market, or as a company); and
- agents representing insurance companies which, for most types of policy, process personal data and in some cases also sensitive personal data.

There are also very many third parties in the insurance records, from the other party in a road traffic accident to legal and other professionals providing litigation-related services.

The usual data protection considerations apply for any record that contains personal data or special categories of personal data: you must not keep the record for longer than is 'necessary' for the purpose(s) for which the data is processed.

10 Insurance products protect policyholders, who may be individuals or organisations (both public and private), against a very wide range of risks associated with people, business and property. There are insurance products that protect policyholders who are individuals, such as travel, health, buildings and contents cover for residential property. And there are insurance products that protect policyholders who are organisations, such as employers' liability, professional indemnity, public liability or marine cover. Insurance products also protect third parties such as motor insurance, where the legal liability of the insurance policyholder is effectively underwritten by the insurance policy. Assurance products (such as life assurance), pensions and other long-term savings products are in some instances provided by the same providers as insurance products. These products may not be covered by a strict definition of insurance and may not be subject to the insurance product lifecycle described below. However, it is may be helpful to group them together as they often involve creating and maintaining records that contain similar personal data and special categories of personal data as 'insurance records'.

Useful starting points to determine if a given record is necessary for the insurance purpose in question are:

- the limitation period for contracts; and
- the fact that the contract of insurance may be a supporting document for tax reasons.

As well as the insurance contract, there will be many associated records that are necessary to enforce rights and fulfil obligations.

Creating an appropriate retention strategy involves assessing if these associated records form part of the overall contract framework between the parties, or are outside it (for example, marketing a policy).

For example, telematics data may form part of the contract or be outside it, depending on exactly what data is captured and how it is used.

It is then necessary to consider if the insurance policy is written on a 'claims made' or on a 'claims arising' (or 'claims occurring') basis.

Under a 'claims made' policy, claims may be made only during the period of time covered by the policy, whereas under a 'claims occurring' policy, claims may be made at any time relating to the risks insured under the policy, even after the policy has expired.

Insurance records relating to claims occurring policies are generally kept for much longer than insurance records relating to claims made policies.

To determine when the limitation period starts to run under a claims occurring policy, this will be later than the policy expiry date.

With regards to limitation periods under English law, actions for breach of contract or on certain torts have a statutory limitation period of six years from the date of the reason for the cause of action[11].

It will also be necessary to consider any applicable regulatory rules and any applicable tax and accounting requirements.

Generally, brokers, agents, insurers and coverholders will tend to keep relevant insurance records until the policyholder can no longer make claims[12] under the terms of the policy. Or, if a claim has been made, until all outstanding claims have settled (either through agreement between the parties or legal proceedings) and no further proceeding (including appeals) are possible.

Similarly, policyholders should keep relevant insurance records for corresponding periods.

The table below sets out recommended retention periods for a select list of insurance records that are likely to contain personal and / or special categories of personal data.

11 Section 2 and 5 of the Limitation Act 1980

12 Note: for the purpose of this section of the guidance 'claims' refers to applications for compensation made by the policy holder under the terms of the insurance policy.

Please note this template is an example. Retention periods need to be internally agreed and justified

Insurance records

Category of data	Paper or electronic	Retention period
Insurance policy, proposal forms, renewal notices and certificates.	Both	Until claims under the policy are barred, all outstanding claims are settled, the policyholder can no longer bring legal proceedings against the insurer or broker and, if legal proceedings have started, the appeals process has been exhausted.
Records relating to the suitability and appropriateness of an insurance-based investment product[13] for the customer.	Both	You must keep records for at least 5 years (Financial Conduct Authority SYSC 9.1.2AR) or if necessary, for the length of the relationship between the insurance intermediary / insurance undertaking and the customer (Article 19 (EU) 2017/2359 and, COBS 9A.4.3 and COBS 10A.7.2A).
Claim documents: records of incidents giving rise to a claim, claim correspondence and records of payouts.	Both	Until claims under the policy are barred, all outstanding claims are settled, the policyholder can no longer bring legal proceedings against the insurer or broker and, if legal proceedings are commenced, the appeals process has been exhausted.
Records relating to Insurance Premium Tax (including policy documents, copies of invoices, credit or debit notes and business and accounting records)	Both	For tax purposes you must keep these records for a period of six years (Regulation 16 of the Insurance Premium Tax Regulations 1994, SI 1994/1774).

13 For a definition of insurance-based investment products see Article 2(1)(17) of Directive (EU) 2016/97.

Continued

Insurance records	
Authority:	Compliance team of the insurer / broker / reinsurer or other party involved.
Information asset owner:	As above.
Location held:	Insurance records kept in line with Article 19 (EU) 2017/2359 or the FCA's Conduct of Business Rules must be held somewhere where they will be accessible by the competent authority. This is generally the party's main place of business. Other insurance records are also likely to be held at the party's main place of business.
Permanent preservation:	No, but as noted above, very long retention periods may in practice apply to many types of insurance record.
Statues that apply:	Commercial considerations, Limitation Act 1980, Commission Regulation (EU) 2017/2359, the Financial Conduct Authority's Conduct of Business Rules, and Insurance Premium Tax Regulations 1994, SI 1994/1774.
Special categories of data:	Yes. Health data will be the most common special category data in insurance records. Some policies (for example, life and health insurance policies) may also contain genetic data (GDPR definition: Article 4(13)).
Criminal convictions data:	Yes. Driving and other offences are often recorded for underwriting purposes. You should not record, keep or use spent convictions in line with the *Rehabilitation of Offenders Act 1974*. There is more guidance on spent convictions at *https://www.unlock.org.uk/*

Customer contract records

In this section we focus on contracts to provide products and services to individuals. Retention periods for this will vary from organisation to organisation, depending on their sector and their products and services.

You should ask yourself why it is necessary to keep customer data after the end of any contract period, or one-off sale.

In most cases you will base your assessment on factors, such as:

- contract obligations which may continue after the sale, such as warranty period;
- customer service and complaints handling;
- records kept for litigation purposes.

Please note this template is an example. Retention periods need to be internally agreed and justified

Customer contract records

Category of data	Paper or electronic	Retention period
Customers (business and consumer)	Both	End of contract plus X months.
Other data subjects identified within customer contracts	Both	End of contract plus X months.
Prospective customers - with marketing consent	Both	The period of marketing consent (e.g. 2 years).
Marketing suppressions (opt-outs)	Both	Minimise and retain permanently.
Call recordings	Electronic	Typically, 24 months or less.
Customer correspondence (letters)	Both	End of contract plus X months.
Customer warranties	Both	Warranty period plus 12 months.
Customer credit records	Both	Period of credit plus 6 years.
Authority:	[To be specified]	
Information asset owner:	[To be specified]	
Location held:	Customer database, marketing database	
Permanent preservation:	Marketing suppressions (opt-outs), which must be minimised	
Statutes that apply:	Consumer Credit Act, Distance Selling Regs, sector-specific laws.	
Special categories of data:	Not normally unless necessary for the contract	

Marketing records

Marketing records may include more data than that to just support marketing activity, such as:

- personal data collected to support the main aim of the organisation, such as product sales.
- funds collected to support charitable causes, or to provide services.

When defining retention periods for marketing records organisations should make sure they consider retention periods set by other purposes for which the same data may be used.

Examples of data elements that are commonly used to support marketing activity include the following.

- Contact details (email, telephone number and postal address).
- Demographic information (date of birth, gender).
- Marketing preferences and permissions (channel specific opt-ins / opt-outs).
- Communication history (which communication were previously sent to the individual but also to which communication the individual has previously responded).
- Variables derived from the individual's transactional history (recency,frequency and monetary value - RFM variables).

From an operational perspective, we can divide marketing activity and the personal data needed to support it into three main areas.

a. Data to contact individuals; (including in profiling individuals to target marketing).
b. Data to support individual requests resulting from marketing activity.
c. Data for measurement and analysis.

Personal data to contact individuals

This data typically includes email address, telephone number and postal address, plus information about previous purchases and demographic information.

Legitimate interests

If the organisation is using the legitimate interest lawful basis and the individual is an existing customer / donor, then they can keep the information for as long as the individual is a customer / donor. This usually means for as long as the individual is actively engaging or has a high likelihood of re-engaging with the organisation.

To determine how likely an individual is to re-engage, the organisation may carry out customer / donor lifecycle analysis, which can provide insight into the typical length of the relationship that individuals have with the organisation.

There are many different ways to approach this analysis, but there is an easy-to-implement methodology in the *UK Data & Marketing Association's (DMA) Advice on Data Retention*.

The organisation will also need to keep the information up to date (GDPR Article 5.1(d)) and can include these reviews with lifecycle analysis.

Consent

If the organisation is using consent as the lawful basis for marketing communications, the retention policy should consider how long the consent is deemed to be valid.

Current DMA guidelines indicate that the maximum time consent is valid in a 'first party' scenario (if the individual is an existing customer / donor) is 24 months after initial collection or any other [later] positive action that indicates an ongoing relationship with the organisation. For example, this could be the individual clicking through from a marketing email to browse the organisation's website.

These are general guidelines and it may be possible for consent to be valid for longer when circumstances justify this, or that it will only be valid for a shorter period of time (such as where the consent was for marketing a particular product or service).

For example, a car company leasing a car to an individual for four years is likely to be able to justify marketing for the length of the contract terms they have with the customer.

Organisations might also want to consider attempting to refresh consent (asking the individual whether they are happy for the organisation to continue to contact them) before the consent 'expiry date'. If the individual re-consents, then the retention 'clock' can be re-set.

If the personal data relates to prospective customers and came from a third party, then there are two scenarios.

- If the contact took place, you should keep the data for a reasonable period of time after the contact to support any further requests from the individual.
- If no contact took place, you should delete the data promptly after the permission to contact expires.

However, if consent is the lawful basis, the DMA has provided the following guidelines.

- For telephone, email, SMS marketing: the maximum time consent is valid is six months after initial collection or any other positive contact.
- For postal marketing: the maximum time consent is valid is 24 months after initial collection or any other positive contact.

***For more information, see the** DMA's GDPR for marketers: Consent and Legitimate Interests*

Personal data to support individual requests

Getting a marketing communication raises people's awareness that an organisation is processing their personal data and can lead individuals to make a rights request.

It is good practice to keep the related personal data for a period of time (such as 6 months) after the contact took place to support any requests. If marketing was done with consent, there is a clear requirement to keep evidence of the consent.

One of the main reasons individuals contact an organisation is to ask them not to send marketing communications in the future (the right to object under GDPR Article 21(2)(a)).

If the individual is an existing customer, it is normally possible to meet the request by updating the marketing preferences in a CRM system.

However, for prospective customers the organisation might not have been planning to keep the personal data beyond a short period after contact, if there was no engagement.

You may get an objection to direct marketing at the same time as a deletion request. In these cases, organisations must decide whether to delete all the individual's data or keep a minimised record to make sure they don't contact the individual in the future, even if the individual sees this as conflicting with the deletion request.

The ICO's guidance states; "an individual can ask you to stop processing their personal data for direct marketing at any time. This includes any profiling of data that is related to direct marketing".

This is an absolute right with no grounds to refuse. Therefore, when you receive an objection to direct marketing, you must stop processing the individual's data for this purpose.

However, this does not automatically mean that you need to delete the individual's personal data and, in most cases, it will be better to suppress their details. Suppression means keeping just enough information about them to make sure you respect their preference not to receive direct marketing.

It is advisable to keep a minimised record on a suppression file until you remove the risk of getting in the individual's contact details again. If you are keeping a suppression file, it is probably worth mentioning it in your privacy notice so your customers and other contacts are aware.

Also see: *ICO guidance on right to object*

Personal data for measurement and analysis

Measuring campaign performance and analysing consumer behaviour are integral parts of marketing activity. To support these activities, it might be necessary to keep the individual's contact details to allow the organisation to link stimulus and response and attribute response to the relevant marketing channel(s).

To reduce the overall retention period of individuals' data, and in particular the data related to those who did not respond to the campaign and are not engaging or likely to re-engage with the organisation, it is advisable to complete these operations as soon as possible after the marketing campaign has finished.

You should delete personal data once it is not required for measurement. However, this does not mean that you should delete all the data collected from the individual during the relationship. A better approach would be to anonymise the data so you can continue to use it for analysis purposes and deliver value to the organisation, while protecting the individual's privacy and complying with data protection regulation.

Below are two sample retention schedules: one created by an organisation in the charity sector and one by a commercial organisation.

Table A: Marketing records in the charity sector

Please note this template is an example. Retention periods need to be internally agreed and justified

Marketing records – charity sector		
Category of data	Paper or electronic	Retention period
Active donor / customer record – record including but not limited to name, date of birth, address, consent and communication preferences, transactions, direct debit and gift / gift aid records, general correspondence and communication history	Both	Lifetime of active interaction with organisation. Interaction may for example include; making a donation, taking part in an event or making a complaint.
Inactive donor / customer record – a record of an individual who has had no active interaction with the organisation	Electronic	7 years from last interaction.
Suppressed record – record of an individual who has exercised their right to object to receiving future communication and for whom no other purpose for holding information is identified.	Electronic	Indefinitely – reviewed every 5 years to make sure suppression and retention remains relevant.
Analytics donor record – record of a donor / customer excluding all personal information (may choose to retain CRM ID and postcode district) which is required to be used for statistical or analytical purposes.	Electronic	Indefinitely subject to review every 5 years to make sure retention remains useful.

Continued

Marketing records – charity sector		
Category of data	Paper or electronic	Retention period
Legacy donor record[1] – record for those individuals who have confirmed their legacy; confirmed their intention to include a legacy; or advised they are thinking about leaving a legacy to the charity in their will.	Electronic	Lifetime of active interaction with organisation plus 20 years (see below notes).
Images, photography, film, case studies and related consent forms linked to the said media coverage for use in marketing materials and campaigns	Electronic	3 years from consent expiry for use in marketing materials.
Media coverage – records held consisting of news stories placed or press coverage received.	Both	Reviewed after 5 years to determine if the coverage is historically important; part of a crisis piece; or relates to an organisational priority that needs keeping for longer.
Authority:	[Compliance Team]	
Information asset owner:	[Director of Marketing / Director of Communications or other relevant position in organisation]	
Location held:	[To be specified]	
Permanent preservation:	No	
Statutes that apply:	None	
Special categories of data:	No	

1 Legacy Fundraising and Records Retention:

Where a charity is a named beneficiary in an individual's will, they may be required to evidence their relationship with the individual. This usually involves showing a pattern of contact, or the details of a relationship, so more than a name, contact details and the fact the individual was a supporter.

A large number of legacy gifts come as a surprise and the number of individuals who leave a gift in their will is generally small compared to the overall size of a charity's donor database.

Therefore, taking into consideration the storage limitation principle, this means that a charity should not keep the records of all donors who have ever interacted with them 'just in case' they leave a legacy in the future.

You need a balanced approach which considers aspects such as:

- lawful bases for processing;
- how much you rely on legacy income;
- how likely is it you will receive legacies from former donors;
- what indication you have of a potential legacy gift; and
- how long ago the donor last interacted with you.

Many charities will identify legacy supporters or carry out specific legacy fundraising / marketing. This provides a possible option for records retention by identifying groups of donors based on their relationship and interaction with the charity.

For example, a legacy pledger is a term used to describe someone who has told the charity they have left them a gift in their will. Therefore, it may be reasonable for a charity to apply a longer retention period to the records for this group of donors to account for the known legacy gift.

In contrast, a legacy enquirer is a term used to describe someone who has asked for information about leaving a legacy, or who is thinking about leaving a gift, but who hasn't confirmed this. For this group of donors you may decide it is reasonable to hold their records longer than other donors based on your knowledge of their interest in legacy fundraising but, as their intention is not as clear, shorter than legacy pledgers.

The Institute of Fundraising have produced *legacy fundraising and data retention guidance* to help you in your decision-making.

Table B: Marketing records in the commercial sector

Please note this template is an example. Retention periods need to be internally agreed and justified

Marketing records – commercial sector		
Category of data	Paper or electronic	Retention period
Personal data used to contact existing customers (this may include email, telephone number, postal address) or select marketing audiences fromthe existing customers (this may include demographic information, marketing preferences and permission, communication history, and variables derived from the individual's transactional)	Electronic	Typically, 12-24 months from last interaction with (depending on context).
Personal data used to contact prospective customers based on consent (this may include email and telephone number) or select audiences from prospective customers for marketing through electronic channels (this may include demographic information, marketing preferences, and communication history)	Electronic	If the contact took place, 3 months from the contact date; if the contact did not take place, 6 months after initial collection.
Personal data used to carry out suppression requests (this may include email, telephone number, and postal address)	Electronic	Until you remove the risk of sourcing the contact details and inadvertently contacting the individual again; please note that you should minimise the record to minimum information necessary to identify the individual for suppression purposes.
Personal data used for campaign performance measurement	Electronic	13 months from the campaign end date (but if you can anonymise the data and it is still useful then for no longer than necessary to anonymise it).

Continued

Marketing records – commercial sector		
Category of data	Paper or electronic	Retention period
Anonymised data used for analytical or statistical purposes	Electronic	Indefinitely (but review every 5 years to make sure retention remains useful, even if anonymised data is out of scope of GDPR).
Images, photography, film, case studies and related consent forms linked to the said media coverage for use in marketing materials and campaigns	Electronic	Typically, 2-3 years from consent expiry for use in marketing materials.
Media coverage – records held consisting of news stories placed or press coverage received.	Electronic or Paper	Typically, review after 3-5 years to determine if the coverage is historically important; part of a crisis piece; or relates to an organisational priority that needs further retention.
Competition and prize draw records, including adverts, rules and, if applicable, official answers to questions set	Both	Date of last event of a competition (close of competition, winner selection, expiry for winner to claim / select prize) plus typically 1-2 years.
Authority:	[Compliance Team]	
Information asset owner:	[Director of Marketing]	
Location held:	[To be specified]	
Permanent preservation:	No	
Statutes that apply:	None	
Special categories of data:	No	

Public domain records

Many organisations collect personal data from public sources, such as data published on websites, social media or from other published documents.

When deciding on an appropriate retention period for this personal data you should consider the purpose for which it was collected and the lawful basis for processing.

It is also wise to consider how the organisation will meet its obligation to notify individuals within a reasonable period after obtaining the personal data, but at the latest within one month (GDPR Article 14).

Organisations will need to consider the period of time for which it is necessary to keep this personal data. For example, where a business captures prospect data from public online sources for marketing purposes under legitimate interests, the legitimate interests assessment should include data retention.

If the organisation is likely to find notifying the individual difficult, the retention period should reflect this. It will be harder to justify keeping personal data longer than one month.

Data used for or created by artificial intelligence

Organisations using artificial intelligence (AI) solutions, including machine learning, need to consider how long to keep the personal data these solutions create.

Here are a few examples from day-to-day life that involve AI.

- Home appliances (such as Amazon Echo, Google Home and British Gas Hive).
- Law enforcement (predictive policing, criminal justice triage, facial recognition-based surveillance).
- Financial services (credit scoring, threat and fraud detection).
- Internet and social media (recommendation engines, predictive text, online search, advertising, content curation and moderation).
- Autonomous machines (robots, drones, vehicles).

Artificial intelligence systems use various forms of input data (which could include personal data) and algorithms (such as regression, neural networks or decision trees) which are used to train different types of models (such as classification, regression or clustering models).

In the development, testing and calibration phases, input data is required to train models and make sure they can successfully perform their function (to predict, classify or cluster). Beyond this, new data is used for the trained model to process 'live' once the model is in use.

Some systems may iteratively and continuously use input data over months or years. Some machines require continual access to high volumes of fresh data to operate effectively. A good example is an IT threat detection system.

High volumes of different personal data may also be necessary to evidence the training process had enough integrity and adequately represented the population on which the system will be used, and so has not introduced unintended statistical bias in the model's output.

How then do you arrive at appropriate data retention decisions?

Consider the same principles as other scenarios when using personal data.

- **Minimise** - effective minimisation reduces the data which is processed and so that is in scope of your data retention policy. Mining unstructured data using machine learning is a current AI application that appears to conflict with this principle.
- **Anonymise / aggregate** – GDPR does not cover data from which no individual can be uniquely identified but it can still be fully effective. For example, smart cities can develop efficient traffic control, identify the best sites for utilities such as hospitals, transport links and civic amenities without needing to process personal data. However, the bar for anonymisation is set extremely high and EU regulators are particularly sceptical that effective anonymisation is possible in many use cases.

Data retention decisions

When considering data retention, an organisation must assess when the personal data used to create or to calibrate AI-based systems will no longer be necessary to keep.

These decisions should have documented policies and justifications. One specific consideration is the that many of the applications continue to evolve.

If the outcome of an AI application has a significant impact on an individual, then you must be able to understand the data that applied at the point in time when that outcome happened.

Depending on the lifecycle of the model, the relevant associated product or service, and the corresponding rights under data protection law, retention periods could vary significantly, but typically vary between 60 days and 2 years.

Future considerations

There are emerging challenges, including whether machine learning models trained on personal data could themselves be categorised as personal data. Although this is not presently the case, it is technically possible to carry out a number of adversarial attacks on machine learning models allowing attackers to reverse engineer personal data. If this becomes a wider concern, the retention cycles for machine learning models may be shorter.

Case study: threat detection systems

Using machine learning to identify internal and external threats, including those by intelligent machines. Threat detection systems use automated gatekeeping measures such as data leakage management, perimeter scanning, and so on. They may identify abnormal patterns which may be the result of a virus or malware. Such systems need to take in vast amounts of data so they can identify normal patterns and trends, so they can identify abnormal behaviours and potential threats. Watching system behaviour using automated checks on performance to identify spikes, persistent or unusual low-level activity for the type of system.

Data minimisation means that although vast amounts of data may be used to create the machine and calibrate the normal patterns, only data which is essential for the purposes is used. In some situations it will not be necessary to keep certain data in the form of personal data once the model is calibrated and used. If you do not need the data for other business purposes, it would be wise for the controller to consider options for destruction, archiving, de-identifying or pseudonymising the data which is no longer necessary.

The data used for an intelligent threat detection system may be real-time, near real time or within a recent operating period (such as within the current working day). You may need to keep this data (perhaps in the form of log files).

Archived records

Archiving under public interest, scientific, historical or for statistical purposes

Organisations may no longer need personal data for operational purposes but may be able to justify keeping it for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes.

You need to assess retention for these purposes on a case-by-case basis and the storage limitation principle applies. Organisations relying on this justification must recognise they cannot start using the data again for another purpose at a later date.

The archiving should not be incompatible with the original purpose. Consider GDPR Article 89, relevant recitals (156-163) and Section 19 and Schedule 2, Part 6 of the Data Protection Act 2018.

You need to make sure there are appropriate safeguards to protect any personal data kept solely for one of these purposes from unauthorised access.

Organisations should consider adopting data minimisation and / or pseudonymisation or anonymisation. Where you can achieve your purpose without identifying individuals you should anonymise the data. If data is not anonymised, review access controls to make sure access is restricted to those who need it for the specified purpose.

Appendix B – glossary of terms

Anonymisation
Anonymisation is the process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified.

Consent
As defined under GDPR Article 4(11) – *'Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.'*

Controller
As defined under GDPR 4(7) - *'Controller means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data; where the purposes and means of processing are determined by EU or Member State laws, the controller (or the criteria for nominating the controller) may be designated by those laws.'*

Deletion
Deletion of data means to remove or erase the data from an electronic file.

Destruction
The process of destroying data so that it is completely unreadable and cannot be accessed or used.

Lawful basis
The term 'Lawful basis' was used in this guidance where possible to emphasise that it is part of the 'lawfulness' requirement under the GDPR and to avoid potential confusion with references to a domestic / national legal basis for public task processing.

Personal data
As defined under GDPR Article 4(1) – '*Personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.'*

Processing
As defined under GDPR Article 4(2) - *"Processing" means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'*

Processor
A defined under GDPR Article 4(8) - "Processor means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.'

Pseudonymisation
As defined under GDPR Article 4(5) - *'pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.'*

Special categories of personal data
GDPR Article 9 defines special categories of data as *'racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.'*

Record of Processing Activities (RoPA)
Under GDPR Article 30 there is a requirement for organisations to keep a detailed record of their processing activities. This document should cover areas such as processing purposes, data sharing and retention. There is a limited exemption for small and medium-sized organisations (with less than 250 employees).

Third party
As defined under GDPR Article 4(10) – *'Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data'*

Copyright and disclaimer

The information provided in this guidance represents the views of the Data Protection Network's Data Retention Working Group.
It does not provide legal advice and cannot be interpreted as offering comprehensive guidance to the General Data Protection Regulation (Regulation (EU) 2016/679) or other statutory measures referred to in the document.

www.dpnetwork.org.uk

DATA PROTECTION NETWORK