General Data Protection Regulation and Start-Ups – What does it mean?

Introduction – What is GDPR and How does it affect you as a start-up 1
Principle 1: Lawfulness, fairness and transparency 2
Principle 2: Purpose limitation 10
Principle 3: Data minimisation 13
Principle 4: Accuracy 15
Principle 5: Storage limitation 18
Principle 6: Integrity and confidentiality (security) 20
Principle 7: Accountability 26

Introduction – What is GDPR and How does it affect you as a start-up

General Data Protection Regulation – GDPR has been on everybody's lips for the past year or so. As it is now becoming Business as Usual, what will it mean for you starting your own business?

The GDPR applies to businesses established in the EU that process personal data of any EU citizens, so far regardless of developments with Brexit. It also applies to organisations outside the EU which offer goods or services inside the EU.

There are a few things to remember, GDPR is Technology neutral, that means it is a way of working with data which you can do irrespective of which technology you use. There is no such as a "blanket compliance" because you will need to take into account national legislation e.g. for taxation. However, the legislator realises that, unless you live in a cage with no human interaction, there is no such thing as complete privacy safety and security. Which is why you as a business owner must document what measures you've set in place to protect the data, and what your plans are to mitigate any damage should you experience a breach. GDPR has a risk-based approach, and the legislators realise that there is no 'one size fits all' solution to information security. It means that what's 'appropriate' for you will depend on your own circumstances, the processing you're doing, and the risks it presents to your organisation. Most organisations must document their processing activities to some extent. Both controllers and processors have their own documentation obligations, but controllers need to keep more extensive records than processors.

That means that you as a start-up should take GDPR into account when starting your business.

Even if you have fewer than 250 employees, the cut-off for GDPR, and highly likely for a start-up, you still need to prove that you take privacy seriously. Complying with the GDPR from the onset will help you as you grow. As a start-up, you need only document processing activities that:

- are not occasional (e.g., are more than just a one-off occurrence or something you do rarely); or
- are likely to result in a risk to the rights and freedoms of individuals (e.g., something that might be intrusive or adversely affect individuals); or
- involve special category data or criminal conviction and offence data

---

If you suffer a breach you must be able to show any investigator or auditor that you have done your utmost to safeguard the data, you are handling. Plans to safeguard data must contain your recovery plans to mitigate any negative outcome of the breach.

Make sure each entry in your database or spreadsheet has only a single purpose for the processing. If you use the same set of data for different types of processing, duplicate the entry and change the purpose bit on each entry. For example, if you use your registered users' email address both as a key to their user accounts and also for some marketing purposes (e.g., finding and following them on LinkedIn), then those are two separate purposes.

But with a bit of planning, you will achieve Privacy by Design, which will give you a competitive edge. Remember: privacy is good for business.

GDPR sets out seven key principles when dealing with personal data:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

Or in other words – only collect what you need, tell the concerned that you collect their data at the time of collection, data must be correct and when you don't need the data - destroy it. Show what measures you've put in place to protect the data, and how to manage if you suffer a breach.

Added to this, you must assign a Data Protection Officer; the person doesn't have to be an employee.

Yes, GDPR compliance is really that simple – common sense put into law.

Principle 1: Lawfulness, fairness and transparency

Lawfulness, fairness and transparency - At a glance

- You must identify valid grounds under the GDPR (known as a 'lawful basis') for collecting and using personal data.
- You must ensure that you do not do anything with the data in breach of any other laws.
- You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
- You must be clear, open and honest with people from the start about how you will use their personal data.

A checklist to achieve Lawfulness, Fairness and Transparency:

Lawfulness

- ☐ We have identified an appropriate lawful basis (or bases) for our processing.
- ☐ If we are processing special category data or criminal offence data, we have identified a condition for processing this type of data.
- ☐ We don't do anything generally unlawful with personal data.

What is lawfulness?

To ensure that the processing of personal data is lawful, you need to identify specific grounds for the processing. This is called a 'lawful basis' for processing, and there are six options which depend on your purpose and your relationship with the individual. There are also specific additional conditions for processing some especially sensitive types of data.

The 6 lawful bases

1. Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
4. Vital interests: processing is necessary to protect someone's life.

5. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

If no lawful basis applies then your processing will be unlawful and in breach of this principle.

Lawfulness also means that you don't do anything with the personal data which is unlawful. This includes statute and common law obligations, whether criminal or civil. If processing involves committing a criminal offence, it will obviously be unlawful. However, processing may also be unlawful if it results in:

- a breach of a duty of confidence;
- your organisation exceeding its legal powers or exercising those powers improperly;
- an infringement of copyright;
- a breach of an enforceable contractual agreement;
- a breach of industry-specific legislation or regulations; or
- a breach of the Human Rights Act 1998.

These are just examples, and this list is not exhaustive. You may need to take your own legal advice on other relevant legal requirements.

If you have processed personal data unlawfully, the GDPR gives individuals the right to erase that data or restrict your processing of it.

Lawful basis for processing - At a glance

- You must have a valid lawful basis in order to process personal data.
- There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.
- Most lawful bases require that processing is 'necessary' for a specific purpose. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.
- You must determine your lawful basis before you begin processing, and you should document it. We have an interactive tool to help you.
- Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason. In particular, you cannot usually swap from consent to a different basis.
- Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.
- If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).
- If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
- If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

Checklist

- ☐ We have reviewed the purposes of our processing activities and selected the most appropriate lawful basis (or bases) for each activity.
- ☐ We have checked that the processing is necessary for the relevant purpose, and are satisfied that there is no other reasonable way to achieve that purpose.
- ☐ We have documented our decision on which lawful basis applies to help us demonstrate compliance.
- ☐ We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.
- ☐ Where we process special category data, we have also identified a condition for processing special category data, and have documented this.
- ☐ Where we process criminal offence data, we have also identified a condition for processing this data, and have documented this.
- ☐ Fairness
- ☐ We have considered how the processing may affect the individuals concerned and can justify any adverse impact.
- ☐ We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.
- ☐ We do not deceive or mislead people when we collect their personal data.

What is fairness?

Fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them. You need to stop and think not just about how you can use personal data, but also about whether you should.

In order to assess whether or not you are processing personal data fairly, you must consider more generally how it affects the interests of the people concerned – as a group and individually. If you have obtained and used the information fairly in relation to most of the people it relates to but unfairly in relation to one individual, there will still be a breach of this principle.

If any aspect of your processing is unfair you will be in breach of this principle – even if you can show that you have a lawful basis for the processing.

Assessing whether you are processing information fairly depends partly on how you obtain it. In particular, if anyone is deceived or misled when the personal data is obtained, then this is unlikely to be fair.

Personal data may sometimes be used in a way that negatively affects an individual without this necessarily being unfair. What matters is whether or not such detriment is justified.

You should also ensure that you treat individuals fairly when they seek to exercise their rights over their data. This ties in with your obligation to facilitate the exercise of individuals' rights.

Transparency

We are open and honest and comply with the transparency obligations of the right to be informed.

What is transparency?

Transparency is fundamentally linked to fairness. Transparent processing is about being clear, open and honest with people from the start about who you are, and how and why you use their personal data.

Transparency is always important, but especially in situations where individuals have a choice about whether they wish to enter into a relationship with you. If individuals know at the outset what you will use their information for, they will be able to make an informed decision about whether to enter into a relationship or perhaps to try to renegotiate the terms of that relationship.

Transparency is important even when you have no direct relationship with the individual and collect their personal data from another source. In some cases, it can be even more important - as individuals may have no idea that you are collecting and using their personal data, and this affects their ability to assert their rights over their data. This is sometimes known as 'invisible processing'.

You must ensure that you tell individuals about your processing in a way that is easily accessible and easy to understand. You must use clear and plain language.

Consent

Consent is by far the most usual of a lawful basis for processing. However, it comes with the same high standards as another basis. As an employer, you should refrain from using consent as a lawful basis, since you will be considered to be in a much stronger position than that of your employee.

At a glance

- The GDPR sets a high standard for consent. But you often won't need consent. If consent is difficult, look for a different lawful basis.
- Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation.
- Check your consent practices and your existing consents. Refresh your consents if they don't meet the GDPR standard.
- Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent.
- Explicit consent requires a very clear and specific statement of consent.
- Keep your consent requests separate from other terms and conditions.
- Be specific and 'granular' so that you get separate consent for separate things. Vague or blanket consent is not enough.
- Be clear and concise.
- Name any third-party controllers who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.
- Keep consent under review, and refresh it if anything changes.
- Avoid making consent to processing a precondition of a service.
- Public authorities and employers will need to take extra care to show that consent is freely given and should avoid over-reliance on consent.

Checklists - Asking for consent

- ☐ We have checked that consent is the most appropriate lawful basis for processing.
- ☐ We have made the request for consent prominent and separate from our terms and conditions.
- ☐ We ask people to positively opt-in.
- ☐ We don't use pre-ticked boxes or any other type of default consent.
- ☐ We use clear, plain language that is easy to understand.
- ☐ We specify why we want the data and what we're going to do with it.
- ☐ We give separate distinct ('granular') options to consent separately to different purposes and types of processing.

- ☐ We name our organisation and any third-party controllers who will be relying on the consent.
- ☐ We tell individuals they can withdraw their consent.
- ☐ We ensure that individuals can refuse to consent without detriment.
- ☐ We avoid making consent a precondition of a service.
- ☐ If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

Recording consent

- ☐ We keep a record of when and how we got consent from the individual.
- ☐ We keep a record of exactly what they were told at the time.
- ☐ Managing consent
- ☐ We regularly review consents to check that the relationship, the processing, and the purposes have not changed.
- ☐ We have processes in place to refresh consent at appropriate intervals, including any parental consents.
- ☐ We consider using privacy dashboards or other preference-management tools as a matter of good practice.
- ☐ We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.
- ☐ We act on the withdrawals of consent as soon as we can. (Be clear about that in any documentation – internal and external.)
- ☐ We do not penalise individuals who wish to withdraw consent.

When is processing 'necessary'?

Many of the lawful bases for processing depend on the processing being “necessary”. This does not mean that processing has to be absolutely essential. However, it must be more than just useful, and more than just standard practice. It must be a targeted and proportionate way of achieving a specific purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means, or by processing fewer data.

It is not enough to argue that processing is necessary because you have chosen to operate your business in a particular way. The question is whether the processing is objectively necessary for the stated purpose, not whether it is a necessary part of your chosen methods.

Why is the lawful basis for processing important?

The first principle requires that you process all personal data lawfully, fairly and in a transparent manner. If no lawful basis applies to your processing, your processing will be unlawful and in breach of the first principle.

Individuals also have the right to erase personal data which has been processed unlawfully.

The individual’s right to be informed under Article 13 and 14 requires you to provide people with information about your lawful basis for processing. This means you need to include these details in your privacy notice.

The lawful basis for your processing can also affect which rights are available to individuals. For example, some rights will not apply:

	Right to Erasure	Risk to Portability	Right to Object
Consent			X But right to withdraw consent
Contract			X
Legal obligation	X	X	X
Vital interests	X	X	x
Public task	X	X	
Legitimate interest		X	

However, an individual always has the right to object to processing for the purposes of direct marketing, whatever lawful basis applies.

The remaining rights are not always absolute, and there are other rights which may be affected in other ways. For example, your lawful basis may affect how provisions relating to automated decisions and profiling apply, and if you are relying on legitimate interests you need more detail in your privacy notice.

How do we decide which lawful basis applies?

This depends on your specific purposes and the context of the processing. You should think about why you want to process the data, and consider which lawful basis best fits the circumstances. The ICO, the UK Information Commissioner's office has an interactive guidance tool that will help you on the first steps to identify which, if any, lawful basis you are working with.

You might consider that more than one basis applies, in which case you should identify and document all of them from the start.

You must not adopt a one-size-fits-all approach. No one basis should be seen as always better, safer or more important than the others, and there is no hierarchy in the order of the list in the GDPR.

Several of the lawful bases relate to a particular specified purpose – a legal obligation, performing a contract with the individual, protecting someone's vital interests, or performing your public tasks. If you are processing for these purposes then the appropriate lawful basis may well be obvious, so it is helpful to consider these first.

In other cases, you are likely to have a choice between using legitimate interests or consent. You need to give some thought to the wider context, including:

- Whom does the processing benefit?
- Would individuals expect this processing to take place?
- What is your relationship with the individual?
- Are you in a position of power over them?
- What is the impact of the processing on the individual?
- Are they vulnerable?
- Are some of the individuals concerned likely to object?
- Are you able to stop the processing at any time on request?

You may prefer to consider legitimate interests as your lawful basis if you wish to keep control over the processing and take responsibility for demonstrating that it is in line with people's reasonable

expectations and wouldn't have an unwarranted impact on them. On the other hand, if you prefer to give individuals full control over and responsibility for their data (including the ability to change their mind as to whether it can continue to be processed), you may want to consider relying on individuals' consent.

Can we change our lawful basis?

You must determine your lawful basis before starting to process personal data. It's important to get this right the first time. If you find at a later date that your chosen basis was actually inappropriate, it will be difficult to simply swap to a different one. Even if a different basis could have applied from the start, retrospectively switching lawful basis is likely to be inherently unfair to the individual and lead to breaches of accountability and transparency requirements.

It is therefore important to thoroughly assess upfront which basis is appropriate and document this. It may be possible that more than one basis applies to the processing because you have more than one purpose, and if this is the case then you should make this clear from the start.

If there is a genuine change in circumstances or you have a new and unanticipated purpose which means there is a good reason to review your lawful basis and make a change, you need to inform the individual and document the change.

What happens if we have a new purpose?

If your purposes change over time or you have a new purpose which you did not originally anticipate, you may not need a new lawful basis as long as your new purpose is compatible with the original purpose.

However, the GDPR specifically says this does not apply to processing based on consent. Consent must always be specific and informed. You need to either get fresh consent which specifically covers the new purpose, or find a different basis for the new purpose. If you do get specific consent for the new purpose, you do not need to show it is compatible.

In other cases, in order to assess whether the new purpose is compatible with the original purpose you should take into account:

- any link between your initial purpose and the new purpose;
- the context in which you collected the data – in particular, your relationship with the individual and what they would reasonably expect;
- the nature of the personal data – e.g. is it special category data or criminal offence data;
- the possible consequences for individuals of the new processing; and
- whether there are appropriate safeguards - e.g. encryption or pseudonymisation.

This list is not exhaustive and what you need to look at depends on the particular circumstances.

As a general rule, if the new purpose is very different from the original purpose, would be unexpected, or would have an unjustified impact on the individual, it is unlikely to be compatible with your original purpose for collecting the data. You need to identify and document a new lawful basis to process the data for that new purpose.

The GDPR specifically says that further processing for the following purposes should be considered to be compatible lawful processing operations:

- archiving purposes in the public interest;
- scientific research purposes; and

- statistical purposes.

There is a link here to the 'purpose limitation' principle in Article 5, which states that "personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".

Even if the processing for a new purpose is lawful, you will also need to consider whether it is fair and transparent, and give individuals information about the new purpose.

How should we document our lawful basis?

The principle of accountability requires you to be able to demonstrate that you are complying with the GDPR, and have appropriate policies and processes. This means that you need to be able to show that you have properly considered which lawful basis applies to each processing purpose and can justify your decision.

You need therefore to keep a record of which basis you are relying on for each processing purpose and a justification for why you believe it applies. There is no standard form for this, as long as you ensure that what you record is sufficient to demonstrate that a lawful basis applies. This will help you comply with accountability obligations, and will also help you when writing your privacy notices.

It is your responsibility to ensure that you can demonstrate which lawful basis applies to the particular processing purpose.

Read the accountability section of this guide for more on this topic. There is also further guidance on documenting consent or legitimate interest.

What do we need to tell people?

You need to include information about your lawful basis (or bases, if more than one applies) in your privacy notice. Under the transparency provisions of the GDPR, the information you need to give people includes:

- your intended purposes for processing the personal data; and
- the lawful basis for the processing.

This applies whether you collect the personal data directly from the individual or you collect their data from another source.

Read the 'right to be informed' section of this guide for more on the transparency requirements of the GDPR.

Principle 2: Purpose limitation

Purpose limitation - At a glance

- ☐ You must be clear about what your purposes for processing are from the start.
- ☐ You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals.
- ☐ You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear basis in law.

Checklist to achieve Purpose limitation

- ☐ We have clearly identified our purpose or purposes for processing.
- ☐ We have documented those purposes.
- ☐ We include details of our purposes in our privacy information for individuals.
- ☐ We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.
- ☐ If we plan to use personal data for a new purpose, we check that this is compatible with our original purpose or we get specific consent for the new purpose.

The purpose limitation principle prevents you from using personal data for new purposes if they are 'incompatible' with your original purpose for collecting the data, but the GDPR contains more detail on assessing compatibility.

The Purpose limitation principle means in practice, that you must:

- ☐ be clear from the outset why you are collecting personal data and what you intend to do with it;
- ☐ comply with your documentation obligations to specify your purposes;
- ☐ comply with your transparency obligations to inform individuals about your purposes; and
- ☐ ensure that if you plan to use or disclose personal data for any purpose that is additional to or different from the originally specified purpose, the new use is fair, lawful and transparent.

Instead of an exemption for research purposes, the GDPR purpose limitation principle specifically says that it does not prevent further processing for:

- ☐ archiving purposes in the public interest;
- ☐ scientific or historical research purposes; or
- ☐ statistical purposes

Why do we need to specify our purposes?

This requirement aims to ensure that you are clear and open about your reasons for obtaining personal data and that what you do with the data is in line with the reasonable expectations of the individuals concerned.

Specifying your purposes from the outset helps you to be accountable for your processing, and helps you avoid 'function creep'. It also helps individuals understand how you use their data, make decisions about whether they are happy to share their details, and assert their rights over data where appropriate. It is fundamental to building public trust in how you use personal data.

If you use data for unfair, unlawful or 'invisible' reasons, it's likely to be a breach of both principles. Specifying your purposes is necessary to comply with your accountability obligations.

How do we specify our purposes?

If you comply with your documentation and transparency obligations, you are likely to comply with the requirement to specify your purposes without doing anything more:

- You need to specify your purpose or purposes for processing personal data within the documentation you are required to keep as part of your records of processing.
- You also need to specify your purposes in your privacy information for individuals.

However, you should also remember that whatever you document, and whatever you tell people, this cannot make fundamentally unfair processing fair and lawful.

If you are a small organisation and you are exempt from some documentation requirements, you may not need to formally document all of your purposes to comply with the purpose limitation principle. Listing your purposes in the privacy information you provide to individuals will be enough. However, it is still a good practice to document all of your purposes.

If you have not provided privacy information because you are only using personal data for an obvious purpose that individuals already know about, the "specified purpose" should be taken to be the obvious purpose.

You should regularly review your processing, documentation and privacy information to check that your purposes have not evolved over time beyond those you originally specified ('function creep').

Once we collect personal data for a specified purpose, can we use it for other purposes?

The GDPR restricts this. In essence, if your purposes change over time or you want to use data for a new purpose which you did not originally anticipate, you can only go ahead if:

- the new purpose is compatible with the original purpose;
- you get the individual's specific consent for the new purpose; or
- you can point to a clear legal provision requiring or allowing the new processing in the public interest – for example, a new function for a public authority.

If your new purpose is compatible, you don't need a new lawful basis for further processing. However, you should remember that if you originally collected the data on the basis of consent, you usually need to get fresh consent to ensure your new processing is fair and lawful.

You also need to make sure that you update your privacy information to ensure that your processing is still transparent.

What is a 'compatible' purpose?

The GDPR specifically says that the following purposes should be considered to be compatible purposes:

- archiving purposes in the public interest;
- scientific or historical research purposes; and
- statistical purposes.

Otherwise, the GDPR says that to decide whether a new purpose is compatible (or as the GDPR says, "not incompatible") with your original purpose you should take into account:

- any link between your original purpose and the new purpose;
- the context in which you originally collected the personal data – in particular, your relationship with the individual and what they would reasonably expect;

- the nature of the personal data – e.g. is it particularly sensitive;
- the possible consequences for individuals of the new processing; and
- whether there are appropriate safeguards - e.g. encryption or pseudonymisation.

As a general rule, if the new purpose is either very different from the original purpose, would be unexpected, or would have an unjustified impact on the individual, it is likely to be incompatible with your original purpose. In practice, you are likely to need to ask for specific consent to use or disclose data for this type of purpose.

There are clear links here with the lawfulness, fairness and transparency principle. In practice, if your intended processing is fair, you are unlikely to breach the purpose limitation principle on the basis of incompatibility.

Principle 3: Data minimisation

This is the first of three principles about data standards, along with accuracy and storage limitation.

Data minimisation - At a glance

You must ensure the personal data you are processing is:

- adequate – sufficient to properly fulfil your stated purpose;
- relevant – has a rational link to that purpose; and
- limited to what is necessary – you do not hold more than you need for that purpose.

Checklist to achieve Data minimisation

- We only collect personal data we actually need for our specified purposes.
- We have sufficient personal data to properly fulfil those purposes.
- We periodically review the data we hold and delete anything we don't need.

What is the data minimisation principle?

You should identify the minimum amount of personal data you need to fulfil your purpose. You should hold that much information, but no more.

The accountability principle means that you need to be able to demonstrate that you have appropriate processes to ensure that you only collect and hold the personal data you need.

Also bear in mind that the GDPR says individuals have the right to complete any incomplete data which is inadequate for your purpose, under the right to rectification. They also have the right to get you to delete any data that is not necessary for your purpose, under the right to erasure (right to be forgotten).

How do we decide what is adequate, relevant and limited?

The GDPR does not define these terms. So, to assess whether you are holding the right amount of personal data, you must first be clear about why you need it.

For special category data or criminal offence data, it is particularly important to make sure you collect and retain only the minimum amount of information.

You may need to consider this separately for each individual, or for each group of individuals sharing relevant characteristics. You should, in particular, consider any specific factors that an individual brings to your attention – for example, as part of an objection, request for rectification of incomplete data, or request for erasure of unnecessary data.

You should periodically review your processing to check that the personal data you hold is still relevant and adequate for your purposes, and delete anything you no longer need.

When could we be processing too much personal data?

You should not have more personal data than you need to achieve your purpose. Nor should the data include irrelevant details.

If you need to process particular information about certain individuals only, you should collect it just for those individuals – the information is likely to be excessive and irrelevant in relation to other people.

You must not collect personal data on the off-chance that it might be useful in the future. However, you may be able to hold information for a foreseeable event that may never occur if you can justify it.

If you are holding more data than is actually necessary for your purpose, this is likely to be unlawful (as most of the lawful bases have a necessity element) as well as a breach of the data minimisation principle. Individuals will also have the right to erasure.

When could we be processing inadequate personal data?

If the processing you carry out is not helping you to achieve your purpose then the personal data you have is probably inadequate. You should not process personal data if it is insufficient for its intended purpose.

Obviously, it makes no business sense to have inadequate personal data – but you must be careful not to go too far the other way and collect more than you need.

What about the adequacy and relevance of opinions?

A record of an opinion is not necessarily inadequate or irrelevant personal data just because the individual disagrees with it or thinks it has not taken account of information, they think is important.

However, in order to be adequate, your records should make clear that it is opinion rather than fact. The record of the opinion (or of the context, it is held in) should also contain enough information to enable a reader to interpret it correctly. For example, it should state the date and the author's name and position.

If an opinion is likely to be controversial or very sensitive, or if it will have a significant impact when used or disclosed, it is even more important to state the circumstances or the evidence it is based on. If a record contains an opinion that summarises more detailed records held elsewhere, you should make this clear.

Principle 4: Accuracy

Accuracy - At a glance

- You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact.
- You may need to keep the personal data updated, although this will depend on what you are using it for.
- If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
- You must carefully consider any challenges to the accuracy of personal data.
- Ensure that the source and status of personal data is clear;
- Consider whether it is necessary to periodically update the information.

Checklist - Accuracy

- We ensure the accuracy of any personal data we create.
- We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data.
- We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary.
- If we need to keep a record of a mistake, we clearly identify it as a mistake.
- Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.
- We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.
- As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data.

There are clear links here to the right to rectification, which gives individuals the right to have inaccurate personal data corrected.

When is personal data 'accurate' or 'inaccurate'?

The GDPR does not define the word 'accurate'. It will usually be obvious whether personal data is accurate.

You must always be clear about what you intend the record of the personal data to show. What you use it for may affect whether it is accurate or not. For example, just because personal data has changed doesn't mean that a historical record is inaccurate – but you must be clear that it is a historical record.

What about records of mistakes?

There is often confusion about whether it is appropriate to keep records of things that happened which should not have happened. Individuals understandably do not want their records to be tarnished by, for example, a penalty or other charge that was later cancelled or refunded.

However, you may legitimately need your records to accurately reflect the order of events – in this example, that a charge was imposed, but later cancelled or refunded. Keeping a record of the mistake and its correction might also be in the individual's best interests.

It is acceptable to keep records of mistakes, provided those records are not misleading about the facts. You may need to add a note to make clear that a mistake was made.

What about the accuracy of opinions?

A record of an opinion is not necessarily inaccurate personal data just because the individual disagrees with it, or it is later proved to be wrong. Opinions are, by their very nature, subjective and not intended to record matters of fact.

However, in order to be accurate, your records must make clear that it is an opinion, and, where appropriate, whose opinion it is. If it becomes clear that an opinion was based on inaccurate data, you should also record this fact in order to ensure your records are not misleading.

If an individual challenge the accuracy of an opinion, it is good practice to add a note recording the challenge and the reasons behind it.

How much weight is actually placed on an opinion is likely to depend on the experience and reliability of the person whose opinion it is, and what they base their opinion on. An opinion formed during a brief meeting will probably be given less weight than one derived from considerable dealings with the individual. However, this is not really an issue of accuracy. Instead, you need to consider whether the personal data is "adequate" for your purposes, in line with the data minimisation principle.

Does personal data always have to be up to date?

This depends on what you use the information for. If you use the information for a purpose that relies on it remaining current, you should keep it up to date. For example, you should update your employee payroll records when there is a pay rise. Similarly, you should update your records for customers' changes of address so that goods are delivered to the correct location.

In other cases, it will be equally obvious that you do not need to update information.

You do not need to update personal data if this would defeat the purpose of the processing. For example, if you hold personal data only for statistical, historical or other research reasons, updating the data might defeat that purpose.

In some cases, it is reasonable to rely on the individual to tell you when their personal data has changed, such as when they change address or other contact details. It may be sensible to periodically ask individuals to update their own details, but you do not need to take extreme measures to ensure your records are up to date unless there is a corresponding privacy risk which justifies this.

However, if an individual informs the organisation of a new address, it should update its records. And if a mailing is returned with the message 'not at this address' marked on the envelope – or any other information comes to light which suggests the address is no longer accurate – the organisation should update its records to indicate that the address is no longer current.

What steps do we need to take to ensure accuracy?

Where you use your own resources to compile personal data about an individual, then you must make sure the information is correct. You should take particular care if the information could have serious implications for the individual. It may be impractical to check the accuracy of personal data someone else provides. In order to ensure that your records are not inaccurate or misleading in this case, you must:

- accurately record the information provided;
- accurately record the source of the information;
- take reasonable steps in the circumstances to ensure the accuracy of the information; and
- carefully consider any challenges to the accuracy of the information.

What is a ‘reasonable step’ will depend on the circumstances and, in particular, the nature of the personal data and what you will use it for. The more important it is that the personal data is accurate, the greater the effort you should put into ensuring its accuracy. So, if you are using the data to make decisions that may significantly affect the individual concerned or others, you need to put more effort into ensuring accuracy. Even if you originally took all reasonable steps to ensure the accuracy of the data, if you later get any new information which suggests it may be wrong or misleading, you should reconsider whether it is accurate and take steps to erase, update or correct it in light of that new information as soon as possible. This may mean you have to get independent confirmation that the data is accurate.

What should we do if an individual challenge the accuracy of their personal data?

If this happens, you should consider whether the information is accurate and, if it is not, you should delete or correct it.

Remember that individuals have the absolute right to have incorrect personal data rectified – see the right to rectification for more information.

Individuals don’t have the right to erasure just because data is inaccurate. However, the accuracy principle requires you to take all reasonable steps to erase or rectify inaccurate data without delay, and it may be reasonable to erase the data in some cases. If an individual asks you to delete inaccurate data it is, therefore, good practice to consider this request.

Principle 5: Storage limitation

The GDPR does not set specific time limits for different types of data. This is up to you and will depend on how long you need the data for your specified purposes.

Storage limitation - At a glance

- You must keep personal data only for as long as you need it.
- You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
- You need a policy setting standard retention periods wherever possible, to comply with documentation requirements.
- You should also periodically review the data you hold, and erase or anonymise it when you no longer need it.
- You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
- You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

Storage limitation - Checklist

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

Why is storage limitation important?

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

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

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

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

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

Do we need a retention policy?

Retention policies or retention schedules list the types of record or information you hold, what you use it for, and how long you intend to keep it. They help you establish and document standard retention periods for different categories of personal data.

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

To comply with documentation requirements, you need to establish and document standard retention periods for different categories of information you hold wherever possible. It is also advisable to have a system for ensuring that your organisation keeps to these retention periods in practice, and for reviewing retention at appropriate intervals. Your policy must also be flexible enough to allow for early deletion if appropriate. For example, if you are not actually using a record, you should reconsider whether you need to retain it.

If you are a small organisation undertaking occasional low-risk processing, you may not need a documented retention policy.

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

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

You can keep personal data indefinitely if you are holding it only for:

- archiving purposes in the public interest;
- scientific or historical research purposes; or
- statistical purposes.

Although the general rule is that you cannot hold personal data indefinitely 'just in case' it might be useful in future, there is an inbuilt exception if you are keeping it for these archiving, research or statistical purposes.

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

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

How does this apply to data sharing?

If you share personal data with other organisations, you should agree between you what happens once you no longer need to share the data.

The organisations involved in an information-sharing initiative may each need to set their own retention periods. However, if you all only hold the data for the purposes of the data-sharing initiative and it is no longer needed for that initiative, then all organisations with copies of the information should delete it.

Principle 6: Integrity and confidentiality (security)

You must ensure that you have appropriate security measures in place to protect the personal data you hold.

This is the 'integrity and confidentiality' principle of the GDPR – also known as the security principle.

Security - at a glance

- A key principle of the GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.
- Doing this requires you to consider things like risk analysis, organisational policies, and physical and technical measures.
- You also have to take into account additional requirements about the security of your processing – and these also apply to data processors.
- You can consider the state of the art and costs of implementation when deciding what measures to take – but they must be appropriate both to your circumstances and the risk your processing poses.
- Where appropriate, you should look to use measures such as pseudonymisation and encryption.
- Your measures must ensure the 'confidentiality, integrity and availability' of your systems and services and the personal data you process within them.
- The measures must also enable you to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.
- You also need to ensure that you have appropriate processes in place to test the effectiveness of your measures and undertake any required improvements.

Checklist – Security

- We undertake an analysis of the risks presented by our processing and use this to assess the appropriate level of security we need to put in place.
- When deciding what measures to implement, we take account of the state of the art and costs of implementation.
- We have an information security policy (or equivalent) and take steps to make sure the policy is implemented.
- Where necessary, we have additional policies and ensure that controls are in place to enforce them.
- We make sure that we regularly review our information security policies and measures and, where necessary, improve them.
- We have put in place basic technical controls.
- We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process.
- We use encryption and/or pseudonymisation where it is appropriate to do so.
- We understand the requirements of confidentiality, integrity and availability for the personal data we process.
- We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.
- We conduct regular testing and reviews of our measures to ensure they remain effective and act on the results of those tests where they highlight areas for improvement.
- Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism.

- We ensure that any data processor we use also implements appropriate technical and organisational measures.

What's new?

The GDPR provides more specifics about what you have to do about the security of your processing and how you should assess your information risk and put appropriate security measures in place.

This means that you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. You should remember that while information security is sometimes considered as cybersecurity (the protection of your networks and information systems from attack), it also covers other things like physical and organisational security measures.

Why should we worry about information security?

Poor information security leaves your systems and services at risk and may cause real harm and distress to individuals – lives may even be endangered in some extreme cases.

Some examples of the harm caused by the loss or abuse of personal data include:

- identity fraud;
- fake credit card transactions;
- targeting of individuals by fraudsters, potentially made more convincing by compromised personal data;
- witnesses put at risk of physical harm or intimidation;
- offenders at risk from vigilantes;
- exposure of the addresses of service personnel, police and prison officers, and those at risk of domestic violence;
- fake applications for tax credits; and
- mortgage fraud.

Although these consequences do not always happen, you should recognise that individuals are still entitled to be protected from less serious kinds of harm, for example, embarrassment or inconvenience.

Information security is important, not only because it is itself a legal requirement, but also because it can support good data governance and help you demonstrate your compliance with other aspects of the GDPR.

What do our security measures need to protect?

The security principle goes beyond the way you store or transmit information. Every aspect of your processing of personal data is covered, not just cybersecurity. This means the security measures you put in place should seek to ensure that:

- the data can be accessed, altered, disclosed or deleted only by those you have authorised to do so
- the data you hold is accurate and complete in relation to why you are processing it; and
- the data remains accessible and usable, i.e., if personal data is accidentally lost, altered or destroyed, you should be able to recover it and therefore prevent any damage or distress to the individuals concerned.

These are known as 'confidentiality, integrity and availability' and under the GDPR, they form part of your obligations.

What level of security is required?

The GDPR does not define the security measures that you should have in place. It requires you to have a level of security that is 'appropriate' to the risks presented by your processing. You need to consider this in relation to the state of the art and costs of implementation, as well as the nature, scope, context and purpose of your processing.

So, before deciding what measures are appropriate, you need to assess your information risk. You should review the personal data you hold and the way you use it in order to assess how valuable, sensitive or confidential it is – as well as the damage or distress that may be caused if the data was compromised.

What organisational measures do we need to consider?

Carrying out an information risk assessment is one example of an organisational measure, but you will need to take other measures as well. You should aim to build a culture of security awareness within your organisation. You should identify a person with day-to-day responsibility for information security within your organisation and make sure this person has the appropriate resources and authority to do their job effectively. That person doesn't have to be hired by your company.

Clear accountability for security will ensure that you do not overlook these issues and that your overall security posture does not become flawed or out of date.

Although an information security policy is an example of an appropriate organisational measure, you may not need a 'formal' policy document or an associated set of policies in specific areas. It depends on your size and the amount and nature of the personal data you process, and the way you use that data. However, having a policy does enable you to demonstrate how you are taking steps to comply with the security principle.

What technical measures do we need to consider?

Technical measures are sometimes thought of like the protection of personal data held in computers and networks. Technical measures include both physical and computer or IT security.

In the IT context, technical measures may sometimes be referred to as 'cybersecurity'. This is a complex technical area that is constantly evolving, with new threats and vulnerabilities always emerging. It may, therefore, be sensible to assume that your systems are vulnerable and take steps to protect them.

Depending on the sophistication of your systems, your usage requirements and the technical expertise of your staff, you may need to obtain specialist information security advice that goes beyond the scope of this guidance. However, it's also the case that you may not need a great deal of time and resources to secure your systems and the personal data they process.

What if we operate in a sector that has its own security requirements?

Some industries have specific security requirements or require you to adhere to certain frameworks or standards. These may be set collectively, for example by industry bodies or trade associations, or could be set by other regulators. If you operate in these sectors, you need to be aware of their requirements, particularly if specific technical measures are specified.

Although following these requirements will not necessarily equate to compliance with the GDPR's security principle, it can be the case that they specify certain measures that you should have, and that those measures contribute to your overall security posture.

What do we do when a data processor is involved?

If one or more organisations process personal data on your behalf, then these are data processors under the GDPR. This can have the potential to cause security problems – as a data controller you are responsible for ensuring compliance with the GDPR and this includes what the processor does with the data. However, in addition to this, the GDPR's security requirements also apply to any processor you use.

This means that:

- you must choose a data processor that provides sufficient guarantees about its security measures;
- your written contract must require the processor to undertake the same security measures that you would have to take if you were doing the processing yourself, and
- you should ensure that your contract includes a requirement that the processor makes available all information necessary to demonstrate compliance. This may include allowing you to audit and inspect the processor, either yourself or an authorised third party.

At the same time, your processor can assist you in ensuring compliance with your security obligations. For example, if you lack the resource or technical expertise to implement certain measures, engaging a processor that has these resources can assist you in making sure personal data is processed securely, provided that your contractual arrangements are appropriate.

Should we use pseudonymisation and encryption?

Pseudonymisation and encryption are specified in the GDPR as two examples of measures that may be appropriate for you to implement. This does not mean that you are obliged to use these measures. It depends on the nature, scope, context and purposes of your processing, and the risks posed to individuals.

What are 'confidentiality, integrity, availability' and 'resilience'?

Collectively known as the 'CIA triad', confidentiality, integrity and availability are the three key elements of information security. If any of the three elements is compromised, then there can be serious consequences, both for you as a data controller, and for the individuals whose data you process.

The information security measures you implement should seek to guarantee all three both for the systems themselves and any data they process.

The CIA triad has existed for a number of years and its concepts are well-known to security professionals.

You are also required to have the ability to ensure the 'resilience' of your processing systems and services. Resilience refers to:

- whether your systems can continue operating under adverse conditions, such as those that may result from a physical or technical incident; and
- your ability to restore them to an effective state.

This refers to things like business continuity plans, disaster recovery, and cyber resilience. Again, there is a wide range of solutions available here, and what is appropriate for you depends on your circumstances.

What are the requirements for restoring availability and access to personal data?

You must have the ability to restore the availability and access to personal data in the event of a physical or technical incident in a 'timely manner'.

The GDPR does not define what a 'timely manner' should be. This, therefore, depends on:

- who you are;
- what systems you have; and
- the risk that may be posed to individuals if the personal data you process is unavailable for a period of time.

The key point is that you have taken this into account during your information risk assessment and selection of security measures. For example, by ensuring that you have an appropriate backup process in place you will have some level of assurance that if your systems do suffer a physical or technical incident you can restore them, and therefore the personal data they hold, as soon as reasonably possible.

Are we required to ensure our security measures are effective?

Yes, the GDPR specifically requires you to have a process for regularly testing, assessing and evaluating the effectiveness of any measures you put in place. What these tests look like, and how regularly you do them, will depend on your own circumstances. However, it's important to note that the requirement in the GDPR concerns your measures in their entirety, therefore whatever 'scope' you choose for this testing should be appropriate to what you are doing, how you are doing it, and the data that you are processing.

Technically, you can undertake this through a number of techniques, such as vulnerability scanning and penetration testing. These are essential 'stress tests' of your network and information systems, which are designed to reveal areas of potential risk and things that you can improve.

In some industries, you are required to undertake tests of security measures on a regular basis. The GDPR now makes this an obligation for all organisations. Importantly, it does not specify the type of testing, nor how regularly you should undertake it. It depends on your organisation and the personal data you are processing.

You can undertake to test internally or externally. Whatever form of testing you undertake, you should document the results and make sure that you act upon any recommendations, or have a valid reason for not doing so, and implement appropriate safeguards. This is particularly important if your testing reveals potential critical flaws that could result in a personal data breach.

What about codes of conduct and certification?

If your security measures include a product or service that adheres to a GDPR code of conduct (once any have been approved) or certification (once any have been issued), you may be able to use this as an element to demonstrate your compliance with the security principle. It is important that you check carefully that the code or certification is appropriately issued in accordance with the GDPR.

What about our staff?

The GDPR requires you to ensure that anyone acting under your authority with access to personal data does not process that data unless you have instructed them to do so. It is therefore vital that your staff understand the importance of protecting personal data, are familiar with your security policy and put its procedures into practice.

You should provide appropriate initial and refresher training, including:

- your responsibilities as a data controller under GDPR;
- staff responsibilities for protecting personal data – including the possibility that they may commit criminal offences if they deliberately try to access or disclose these data without authority;
- the proper procedures to identify callers;
- the dangers of people trying to obtain personal data by deception (e.g. by pretending to be the individual whom the data concerns, or enabling staff to recognise 'phishing' attacks), or by persuading your staff to alter information when they should not do so; and
- any restrictions you place on the personal use of your systems by staff (e.g. to avoid virus infection or spam).

Your staff training will only be effective if the individuals delivering it are themselves reliable and knowledgeable.

Principle 7: Accountability

The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles.

You must have appropriate measures and records in place to be able to demonstrate your compliance. Accountability is not just about being answerable to the regulator; you must also demonstrate your compliance to individuals. Amongst other things, individuals have the right to be informed about what personal data you collect, why you use it and whom you share it with. Additionally, if you use techniques such as artificial intelligence and machine learning to make decisions about people, in certain cases individuals have the right to hold you to account by requesting explanations of those decisions and contesting them. You, therefore, need to find effective ways to provide information to people about what you do with their personal data and explain and review automated decisions.

The obligations that accountability places on you are ongoing – you cannot simply sign off a particular processing operation as 'accountable' and move on. You must review the measures you implement at appropriate intervals to ensure that they remain effective. You should update measures that are no longer fit for purpose. If you regularly change what you do with personal data or the types of information that you collect, you should review and update your measures frequently, remembering to document what you do and why.

Accountability - At a glance

- Accountability is one of the data protection principles - it makes you responsible for complying with the GDPR and says that you must be able to demonstrate your compliance.
- You need to put in place appropriate technical and organisational measures to meet the requirements of accountability.
- There are a number of measures that you can, and in some cases must take including:
    - adopting and implementing data protection policies;
    - taking a 'data protection by design and default' approach;
    - putting written contracts in place with organisations that process personal data on your behalf;
    - maintaining documentation of your processing activities;
    - implementing appropriate security measures;
    - recording and, where necessary, reporting personal data breaches;
    - carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
    - appointing a data protection officer; and
    - adhering to relevant codes of conduct and signing up to certification schemes.
- Accountability obligations are ongoing. You must review and, where necessary, update the measures you put in place.
- If you implement a privacy management framework this can help you embed your accountability measures and create a culture of privacy across your organisation.
- Being accountable can help you to build trust with individuals and may help you mitigate enforcement action.

Checklist

- We take responsibility for complying with the GDPR, at the highest management level and throughout our organisation.
- We keep evidence of the steps we take to comply with the GDPR.

- We put in place appropriate technical and organisational measures, such as:
    - adopting and implementing data protection policies (where proportionate);
    - taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;
    - putting written contracts in place with organisations that process personal data on our behalf;
    - maintaining documentation of our processing activities;
    - implementing appropriate security measures;
    - recording and, where necessary, reporting personal data breaches;
    - carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
    - appointing a data protection officer (where necessary); and
    - adhering to relevant codes of conduct and signing up to certification schemes (where possible).
- We review and update our accountability measures at appropriate intervals.

What's new under the GDPR?

One of the biggest changes introduced by the GDPR is around accountability – a new data protection principle that says organisations are responsible for and must be able to demonstrate, compliance with the other principles.

You now need to be proactive about data protection and evidence the steps you take to meet your obligations and protect people's rights.

What is accountability?

There are two key elements. First, the accountability principle makes it clear that you are responsible for complying with the GDPR. Second, you must be able to demonstrate your compliance.

Why is accountability important?

Taking responsibility for what you do with personal data, and demonstrating the steps you have taken to protect people's rights not only results in better legal compliance, it also offers you a competitive edge. Accountability is a real opportunity for you to show, and prove, how you respect people's privacy. This can help you to develop and sustain people's trust.

Furthermore, if something does go wrong, then being able to show that you actively considered the risks and put in place measures and safeguards can help you provide mitigation against any potential enforcement action. On the other hand, if you can't show good data protection practices, it may leave you open to fines and reputational damage.

What do we need to do?

Accountability is not a box-ticking exercise. Being responsible for compliance with the GDPR means that you need to be proactive and organised about your approach to data protection while demonstrating your compliance means that you must be able to evidence the steps you take to comply.

To achieve this, if you are a larger organisation you may choose to put in place a privacy management framework. This can help you create a culture of commitment to data protection, by embedding systematic and demonstrable compliance across your organisation

If you are a smaller organisation you will most likely benefit from a smaller scale approach to accountability. Amongst other things you should:

- ensure a good level of understanding and awareness of data protection amongst your staff;
- implement comprehensive but proportionate policies and procedures for handling personal data; and
- keep records of what you do and why.

Should we implement data protection policies?

For many organisations, putting in place relevant policies is a fundamental part of their approach to data protection compliance. The GDPR explicitly says that where proportionate, implementing data protection policies is one of the measures you can take to ensure, and demonstrate compliance.

What you have policies for, and their level of detail depends on what you do with personal data. If, for instance, you handle large volumes of personal data or particularly sensitive information such as special category data, then you should take greater care to ensure that your policies are robust and comprehensive.

As well as drafting data protection policies, you should also be able to show that you have implemented and adhered to them.

Some measures you are obliged to take and some are voluntary. It will differ depending on what personal data you have and what you do with it. These measures can form the basis of your programme controls if you opt to put in place a privacy management framework across your organisation.

Should we adopt a 'data protection by design and default' approach?

Privacy by design has long been seen as a good practice approach when designing new products, processes and systems that use personal data. Under the heading 'data protection by design and by default', the GDPR legally requires you to take this approach.

Data protection by design and default is an integral element of being accountable. It is about embedding data protection into everything you do, throughout all your processing operations. The GDPR suggests measures that may be appropriate such as minimising the data you collect, applying pseudonymisation techniques, and improving security features.

Do we need to use contracts?

Whenever a controller uses a processor to handle personal data on their behalf, it needs to put in place a written contract that sets out each party's responsibilities and liabilities.

Contracts must include certain specific terms as a minimum, such as requiring the processor to take appropriate measures to ensure the security of processing and obliging it to assist the controller in allowing individuals to exercise their rights under the GDPR.

What documentation should we maintain?

Most organisations are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention.

Documenting this information is a great way to take stock of what you do with personal data. Knowing what information, you have, where it is and what you do with it makes it much easier for you to comply with other aspects of the GDPR such as making sure that the information you hold about people is accurate and secure.

As well as your record of processing activities under Article 30, you also need to document other things to show your compliance with the GDPR. For instance, you need to keep records of consent and any personal data breaches.

What security measures should we put in place?

The GDPR repeats the requirement to implement technical and organisational measures to comply with the GDPR in the context of security. It says that these measures should ensure a level of security appropriate to the risk.

You need to implement security measures if you are handling any type of personal data, but what you put in place depends on your particular circumstances. You need to ensure the confidentiality, integrity and availability of the systems and services you use to process personal data.

Amongst other things, this may include information security policies, access controls, security monitoring, and recovery plans.

How do we record and report personal data breaches?

You must report certain types of personal data breach to the relevant supervisory authority, and in some circumstances, to the affected individuals as well.

Additionally, the GDPR says that you must keep a record of any personal data breaches, regardless of whether you need to report them or not.

You need to be able to detect, investigate, report (both internally and externally) and document any breaches. Having robust policies, procedures and reporting structures help you do this.

Should we carry out data protection impact assessments (DPIAs)?

A DPIA is an essential accountability tool and a key part of taking a data protection by design approach to what you do. It helps you to identify and minimise the data protection risks of any new projects you undertake.

A DPIA is a legal requirement before carrying out processing likely to result in high risk to individuals' interests.

When done properly, a DPIA helps you assess how to comply with the requirements of the GDPR, while also acting as documented evidence of your decision-making and the steps you took.

Should we assign a data protection officer (DPO)?

Some organisations are required to appoint a DPO. A DPO's tasks include advising you about the GDPR, monitoring compliance and training staff.

Your DPO must report to your highest level of management, operate independently, and have adequate resources to carry out their tasks.

Even if you're not obliged to appoint a DPO, it is very important that you have sufficient staff, skills, and appropriate reporting structures in place to meet your obligations under the GDPR.

Should we adhere to codes of conduct and certification schemes?

Under the GDPR, trade associations and representative bodies may draw up codes of conduct covering topics such as fair and transparent processing, pseudonymisation, and the exercise of people's rights.

In addition, supervisory authorities or accredited certification bodies can issue a certification of the data protection compliance of products and services.

Both codes of conduct and certification are voluntary, but they are an excellent way of verifying and demonstrating that you comply with the GDPR.

Who is Exempt from GDPR?

There are limited GDPR exemptions related to the processing of personal data as detailed below:

- When data are processed during the course of an activity that falls outside of the law of the European Union
- GDPR does not apply to individuals that process data for personal or household activity
- GDPR does not apply to government agencies and law enforcement when data are collected and processed for the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties or for preventing threats to public safety
- GDPR does not apply to the processing of personal data by Member States for activities under the scope of Chapter 2, Title V, of the Treaty on European Union.