Data protection

Guide to the General Data Protection Regulation (GDPR)

ico.
Information Commissioner's Office

Introduction 3
What's new 4
Key definitions 7
Principles 9
Lawful basis for processing 10
Consent 20
Contract 25
Legal obligation 29
Vital interests 33
Public task 36
Legitimate interests 40
Special category data 46
Criminal offence data 49
Individual rights 51
Right to be informed 52
Right of access 59
Right to rectification 61
Right to erasure 67
Right to restrict processing 73
Right to data portability 79
Right to object 90
Rights related to automated decision making including profiling 92
Accountability and governance 99
Contracts 109
Documentation 114
Data protection by design and default 119
Data protection impact assessments 120
Data protection officers 127
Codes of conduct and certification 135
Guide to the data protection fee 138
Security 139
International transfers 151
Personal data breaches 154
Exemptions 162
Applications 163
Children 164

Introduction

Introduction

The Guide to the GDPR explains the provisions of the GDPR to help organisations comply with its requirements. It is for those who have day-to-day responsibility for data protection.

This is a living document and we are working to expand it in key areas. It includes links to relevant sections of the GDPR itself, to other ICO guidance and to guidance produced by the EU's Article 29 Working Party. The Working Party includes representatives of the data protection authorities from each EU member state, and the ICO is the UK's representative.

Alongside the Guide to the GDPR, we have produced a number of tools to help organisations to prepare for the GDPR:

Further Reading

GDPR: 12 steps to take now
External link

Data protection self assessment toolkit
For organisations

What's new

We will update this page monthly to highlight and link to what's new in our Guide to the GDPR.

May 2018

We have expanded the page on the right to data portability.

April 2018

We have expanded the page on Accountability and governance.

We have expanded the page on Security.

We have updated all of the lawful basis pages to include a link to the lawful basis interactive guidance tool.

March 2018

We have published detailed guidance on DPIAs for consultation. The consultation will end on 13 April 2018. We have also updated the guide page on DPIAs to include the guide level content from the detailed guidance.

We have published detailed guidance on legitimate interests.

We have expanded the pages on:

- Data protection impact assessments
- Data protection officers
- The right to be informed
- The right to erasure
- The right to rectification
- The right to restrict processing

February 2018

The consultation period for the Article 29 Working party guidelines on consent has now ended and comments are being reviewed. The latest timetable is for the guidelines to be finalised for adoption on 10-11 April.

The consultation period for the Article 29 Working Party guidelines on transparency has now ended.

Following the consultation period, the Article 29 Working Party has adopted final guidelines on Automated individual decision-making and Profiling and personal data breach notification. These have been added to the Guide.

We have published our Guide to the data protection fee.

We have updated the page on Children to include the guide level content from the detailed guidance on Children and the GDPR which is out for public consultation.

January 2018

We have published more detailed guidance on documentation.

We have expanded the page on personal data breaches.

We have also added four new pages in the lawful basis section, covering contract, legal obligation, vital interests and public task.

December 2017

We have published detailed guidance on Children and the GDPR for public consultation. The consultation closes on 28 February 2018.

The sections on Lawful basis for processing and Rights related to automated individual decision making including profiling contain new expanded guidance. We have updated the section on Documentation with additional guidance and documentation templates. We have also added new sections on legitimate interests, special category data and criminal offence data, and updated the section on consent.

The Article 29 Working Party has published the following guidance, which is now included in the Guide.

- Consent
- Transparency

It is inviting comments on these guidelines until 23 January 2018.

The consultation for the Article 29 Working Party guidelines on breach notification and automated decision-making and profiling ended on 28 November. We are reviewing the comments received together with other members of the Article 29 Working Party and expect the guidelines to be finalised in early 2018.

November 2017

The Article 29 Working Party has published guidelines on imposing administrative fines.

We have replaced the Overview of the GDPR with the Guide to the GDPR. The Guide currently contains similar content to the Overview, but we have expanded the sections on Consent and Contracts and Liabilities on the basis of the guidance on these topics which we have previously published for consultation.

The Guide to the GDPR is not yet a finished product; it is a framework on which we will build upcoming GDPR guidance and it reflects how future GDPR guidance will be presented. We will be publishing more detailed guidance on some topics and we will link to these from the Guide. We will do the same for guidelines from the Article 29 Working Party.

October 2017

The Article 29 Working Party has published the following guidance, which is now included in our overview.

- Breach notification
- Automated individual decision-making and Profiling

The Article 29 Working Party has also adopted guidelines on administrative fines and these are expected to be published soon.

In the Rights related to automated decision making and profiling we have updated the next steps for the ICO.

In the Key areas to consider we have updated the next steps in regard to the ICO's consent guidance.

The deadline for responses to our draft GDPR guidance on contracts and liabilities for controllers and processors has now passed. We are analysing the feedback and this will feed into the final version.

September 2017

We have put out for consultation our draft GDPR guidance on contracts and liabilities for controllers and processors.

July 2017

In the Key areas to consider we have updated the next steps in regard to the ICO's consent guidance and the Article 29 Working Party's Europe-wide consent guidelines.

June 2017

The Article 29 Working Party's consultation on their guidelines on high risk processing and data protection impact assessments closed on 23 May. We await the adoption of the final version.

May 2017

We have updated our GDPR 12 steps to take now document.

We have added a Getting ready for GDPR checklist to our self-assessment toolkit.

April 2017

We have published our profiling discussion paper for feedback.

March 2017

We have published our draft consent guidance for public consultation.

January 2017

Article 29 have published the following guidance, which is now included in our overview:

- Data portability
- Lead supervisory authorities
- Data protection officers

Key definitions

Who does the GDPR apply to?

- The GDPR applies to 'controllers' **and** 'processors'.
- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.
- If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.
- However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.
- The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.
- The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

Further Reading

Relevant provisions in the GDPR - Articles 3, 28-31 and Recitals 22-25, 81-82
External link

What information does the GDPR apply to?

- **Personal data**

  The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

  This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

  The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

  Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

- **Sensitive personal data**

  The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9).

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

Further Reading

Relevant provisions in the GDPR - Articles 2, 4, 9, 10 and Recitals 1, 2, 26, 51
External link

Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of the GDPR requires that personal data shall be:

> "a) processed lawfully, fairly and in a transparent manner in relation to individuals;
>
> b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
>
> c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
>
> d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
>
> 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
>
> f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that:

> "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Further Reading

Relevant provisions in the GDPR - see Article 5 and Recital 39
External link

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’. 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. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason.
- 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.

In brief

- What's new?
- Why is the lawful basis for processing important?
- What are the lawful bases?
- When is processing 'necessary'?
- How do we decide which lawful basis applies?
- When should we decide on our lawful basis?
- What happens if we have a new purpose?
- How should we document our lawful basis?
- What do we need to tell people?
- What about special category data?
- What about criminal conviction data?

What's new?

The requirement to have a lawful basis in order to process personal data is not new. It replaces and mirrors the previous requirement to satisfy one of the 'conditions for processing' under the Data Protection Act 1998 (the 1998 Act). However, the GDPR places more emphasis on being accountable for and transparent about your lawful basis for processing.

The six lawful bases for processing are broadly similar to the old conditions for processing, although there are some differences. You now need to review your existing processing, identify the most appropriate lawful basis, and check that it applies. In many cases it is likely to be the same as your existing condition for processing.

The biggest change is for public authorities, who now need to consider the new 'public task' basis first for most of their processing, and have more limited scope to rely on consent or legitimate interests.

You can choose a new lawful basis if you find that your old condition for processing is no longer appropriate under the GDPR, or decide that a different basis is more appropriate. You should try to get this right first time. Once the GDPR is in effect, it will be much harder to swap between lawful bases at will if you find that your original basis was invalid. You will be in breach of the GDPR if you did not clearly identify the appropriate lawful basis (or bases, if more than one applies) from the start.

The GDPR brings in new accountability and transparency requirements. You should therefore make sure you clearly document your lawful basis so that you can demonstrate your compliance in line with Articles 5(2) and 24.

You must now inform people upfront about your lawful basis for processing their personal data. You need therefore to communicate this information to individuals by 25 May 2018, and ensure that you include it in all future privacy notices.

Further Reading

Relevant provisions in the GDPR - See Article 6 and Recital 171, and Article 5(2)
External link

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. Processing is only lawful if you have a lawful basis under Article 6. And to comply with the accountability principle in Article 5(2), you must be able to demonstrate that a lawful basis applies.

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	Right to portability	Right to object
Consent			✘ but right to withdraw consent
Contract			✘
Legal obligation	✘	✘	✘
Vital interests		✘	✘
Public task	✘	✘	
Legitimate interests		✘	

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 to comply with the right to be informed.

Please read the section of this Guide on individuals' rights for full details.

Further Reading

Relevant provisions in the GDPR - See Article 6 and Recitals 39, 40, and Chapter III (Rights of the data subject)

External link

What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) 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.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) 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.

(f) 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.)

For more detail on each lawful basis, read the relevant page of this guide.

Further Reading

> Relevant provisions in the GDPR - See Article 6(1), Article 6(2) and Recital 40
> External link

When is processing 'necessary'?

Many of the lawful bases for processing depend on the processing being "necessary". This does not mean that processing always has to be essential. However, it must be a targeted and proportionate way of achieving the purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means.

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 a necessary for the stated purpose, not whether it is a necessary part of your chosen method of pursuing that purpose.

How do we decide which lawful basis applies?

This depends on your specific purposes and the context of the processing. You should consider which lawful basis best fits the circumstances. 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.

You may need to consider a variety of factors, including:

- What is your purpose – what are you trying to achieve?
- Can you reasonably achieve it in a different way?
- Do you have a choice over whether or not to process the data?
- Are you a public authority?

Several of the lawful bases relate to a particular specified purpose – a legal obligation, 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.

If you are a public authority and can demonstrate that the processing is to perform your tasks as set down in UK law, then you are able to use the public task basis. If not, you may still be able to consider consent or legitimate interests in some cases, depending on the nature of the processing and your relationship with the individual. There is no absolute ban on public authorities using consent or legitimate interests as their lawful basis, but the GDPR does restrict public authorities' use of these two bases.

The Data Protection Bill will define 'public authority' and the final text of those provisions may also have some impact here. We will publish more guidance on the effect of relevant Bill provisions when they are finalised.

Example

A university that wants to process personal data may consider a variety of lawful bases depending on what it wants to do with the data.

Universities are likely to be classified as public authorities, so the public task basis is likely to apply to much of their processing, depending on the detail of their constitutions and legal powers. If the processing is separate from their tasks as a public authority, then the university may instead wish to consider whether consent or legitimate interests are appropriate in the particular circumstances, considering the factors set out below. For example, a University might rely on public task for processing personal data for teaching and research purposes; but a mixture of legitimate interests and consent for alumni relations and fundraising purposes.

The university however needs to consider its basis carefully – it is the controller's responsibility to be able to demonstrate which lawful basis applies to the particular processing purpose.

If you are processing for purposes other than legal obligation, contract, vital interests or public task, then the appropriate lawful basis may not be so clear cut. In many 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:

- Who 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.

When should we decide on our lawful basis?

You must determine your lawful basis before starting to process personal data. It's important to get this right 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.

Example

A company decided to process on the basis of consent, and obtained consent from individuals. An individual subsequently decided to withdraw their consent to the processing of their data, as is their right. However, the company wanted to keep processing the data so decided to continue the processing on the basis of legitimate interests.

Even if it could have originally relied on legitimate interests, the company cannot do so at a later date – it cannot switch basis when it realised that the original chosen basis was inappropriate (in this case, because it did not want to offer the individual genuine ongoing control). It should have made clear to the individual from the start that it was processing on the basis of legitimate interests. Leading the individual to believe they had a choice is inherently unfair if that choice will be irrelevant. The company must therefore stop processing when the individual withdraws consent.

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.

Further Reading

Relevant provisions in the GDPR - See Article 6(1) and Recitals 39 and 40
External link

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 – eg is it special category data or criminal offence data;
- the possible consequences for individuals of the new processing; and
- whether there are appropriate safeguards - eg 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.

Further Reading

Relevant provisions in the GDPR - See Article 6(4), Article 5(1)(b) and Recital 50, Recital 61
External link

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 interests assessments in the relevant pages of the guide.

Further Reading

Relevant provisions in the GDPR - See Articles 5(2) and 24
External link

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.

Further Reading

Relevant provisions in the GDPR - See Article 13(1)(c), Article 14(1)(c) and Recital 39
External link

What about special category data?

If you are processing special category data, you need to identify both a lawful basis for processing and a special category condition for processing in compliance with Article 9. You should document both your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability.

Further guidance can be found in the section on special category data.

What about criminal offence data?

If you are processing data about criminal convictions, criminal offences or related security measures,

you need both a lawful basis for processing and a separate condition for processing this data in compliance with Article 10. You should document both your lawful basis for processing and your criminal offence data condition so that you can demonstrate compliance and accountability.

Further guidance can be found in the section on criminal offence data.

In more detail – ICO guidance

We have produced the lawful basis interactive guidance tool, to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

Consent

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 withdrawals of consent as soon as we can.

☐ We don’t penalise individuals who wish to withdraw consent.

In brief

- What's new?
- Why is consent important?
- When is consent appropriate?

- What is valid consent?
- How should we obtain, record and manage consent?

What's new?

The GDPR sets a high standard for consent, but the biggest change is what this means in practice for your consent mechanisms.

The GDPR is clearer that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

You must keep clear records to demonstrate consent.

The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.

Public authorities, employers and other organisations in a position of power may find it more difficult to show valid freely given consent.

You need to review existing consents and your consent mechanisms to check they meet the GDPR standard. If they do, there is no need to obtain fresh consent.

Why is consent important?

Consent is one lawful basis for processing, and explicit consent can also legitimise use of special category data. Consent may also be relevant where the individual has exercised their right to restriction, and explicit consent can legitimise automated decision-making and overseas transfers of data.

Genuine consent should put individuals in control, build trust and engagement, and enhance your reputation.

Relying on inappropriate or invalid consent could destroy trust and harm your reputation – and may leave you open to large fines.

When is consent appropriate?

Consent is one lawful basis for processing, but there are alternatives. Consent is not inherently better or more important than these alternatives. If consent is difficult, you should consider using an alternative.

Consent is appropriate if you can offer people real choice and control over how you use their data, and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair.

If you make consent a precondition of a service, it is unlikely to be the most appropriate lawful basis.

Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent unless they are confident they can demonstrate it is freely given.

What is valid consent?

Consent must be freely given; this means giving people genuine ongoing choice and control over how you use their data.

Consent should be obvious and require a positive action to opt in. Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly.

Consent must specifically cover the controller's name, the purposes of the processing and the types of processing activity.

Explicit consent must be expressly confirmed in words, rather than by any other positive action.

There is no set time limit for consent. How long it lasts will depend on the context. You should review and refresh consent as appropriate.

How should we obtain, record and manage consent?

Make your consent request prominent, concise, separate from other terms and conditions, and easy to understand. Include:

- the name of your organisation;
- the name of any third party controllers who will rely on the consent;
- why you want the data;
- what you will do with it; and
- that individuals can withdraw consent at any time.

You must ask people to actively opt in. Don't use pre-ticked boxes, opt-out boxes or other default settings. Wherever possible, give separate ('granular') options to consent to different purposes and different types of processing.

Keep records to evidence consent – who consented, when, how, and what they were told.

Make it easy for people to withdraw consent at any time they choose. Consider using preference-management tools.

Keep consents under review and refresh them if anything changes. Build regular consent reviews into your business processes.

Further Reading

Relevant provisions in the GDPR - See Articles 4(11), 6(1)(a) 7, 8, 9(2)(a) and Recitals 32, 38, 40, 42, 43, 171
External link

In more detail - ICO guidance

We will be publishing our more detailed guidance on consent shortly.

We have produced an interactive guidance tool to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

In more detail - Article 29

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 adopted Guidelines on consent on 10 April 2018.

Contract

At a glance

- You can rely on this lawful basis if you need to process someone's personal data:
  - to fulfil your contractual obligations to them; or
  - because they have asked you to do something before entering into a contract (eg provide a quote).
- The processing must be necessary. If you could reasonably do what they want without processing their personal data, this basis will not apply.
- You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning.

In brief

- What's new?
- What does the GDPR say?
- When is the lawful basis for contracts likely to apply?
- When is processing 'necessary' for a contract?
- What else should we consider?

What's new?

Very little. The lawful basis for processing necessary for contracts is almost identical to the old condition for processing in paragraph 2 of Schedule 2 of the 1998 Act.

You need to review your existing processing so that you can document where you rely on this basis and inform individuals. But in practice, if you are confident that your existing approach complied with the 1998 Act, you are unlikely to need to change your existing basis for processing.

What does the GDPR say?

Article 6(1)(b) gives you a lawful basis for processing where:

> "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"

When is the lawful basis for contracts likely to apply?

You have a lawful basis for processing if:

- you have a contract with the individual and you need to process their personal data to comply with your obligations under the contract.
- you haven't yet got a contract with the individual, but they have asked you to do something as a first step (eg provide a quote) and you need to process their personal data to do what they ask.

It does not apply if you need to process one person's details but the contract is with someone else.

It does not apply if you take pre-contractual steps on your own initiative or at the request of a third party.

Example

An individual shopping around for car insurance requests a quotation. The insurer needs to process certain data in order to prepare the quotation, such as the make and age of the car.

Note that, in this context, a contract does not have to be a formal signed document, or even written down, as long as there is an agreement which meets the requirements of contract law. Broadly speaking, this means that the terms have been offered and accepted, you both intend them to be legally binding, and there is an element of exchange (usually an exchange of goods or services for money, but this can be anything of value). However, this is not a full explanation of contract law, and if in doubt you should seek your own legal advice.

When is processing 'necessary' for a contract?

'Necessary' does not mean that the processing must be essential for the purposes of performing a contract or taking relevant pre-contractual steps. However, it must be a targeted and proportionate way of achieving that purpose. This lawful basis does not apply if there are other reasonable and less intrusive ways to meet your contractual obligations or take the steps requested.

The processing must be necessary to deliver your side of the contract with this particular person. If the processing is only necessary to maintain your business model more generally, this lawful basis will not apply and you should consider another lawful basis, such as legitimate interests.

Example

When a data subject makes an online purchase, a controller processes the address of the individual in order to deliver the goods. This is necessary in order to perform the contract.

However, the profiling of an individual's interests and preferences based on items purchased is not necessary for the performance of the contract and the controller cannot rely on Article 6(1)(b) as the lawful basis for this processing. Even if this type of targeted advertising is a useful part of your customer relationship and is a necessary part of your business model, it is not necessary to perform the contract itself.

This does not mean that processing which is not necessary for the contract is automatically unlawful, but rather that you need to look for a different lawful basis.

What else should we consider?

If the processing is necessary for a contract with the individual, processing is lawful on this basis and you do not need to get separate consent.

If processing of special category data is necessary for the contract, you also need to identify a separate condition for processing this data. Read our guidance on special category data for more information.

If the contract is with a child under 18, you need to consider whether they have the necessary competence to enter into a contract. If you have doubts about their competence, you may wish to consider an alternative basis such as legitimate interests, which can help you to demonstrate that the child's rights and interests are properly considered and protected. Read our guidance on children and the GDPR for more information.

If the processing is not necessary for the contract, you need to consider another lawful basis such as legitimate interests or consent. Note that if you want to rely on consent you will not generally be able to make the processing a condition of the contract. Read our guidance on consent for more information.

If you are processing on the basis of contract, the individual's right to object and right not to be subject to a decision based solely on automated processing will not apply. However, the individual will have a right to data portability. Read our guidance on individual rights for more information.

Remember to document your decision that processing is necessary for the contract, and include information about your purposes and lawful basis in your privacy notice.

Further Reading

Relevant provisions in the GDPR - See Article 6(1)(b) and Recital 44
External link

In more detail - ICO guidance

We have produced the lawful basis interactive guidance tool, to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

Legal obligation

At a glance

- You can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation.
- This does not apply to contractual obligations.
- The processing must be necessary. If you can reasonably comply without processing the personal data, this basis does not apply.
- You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning.
- You should be able to either identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out your obligation.

In brief

- What's new?
- What does the GDPR say?
- When is the lawful basis for legal obligations likely to apply?
- When is processing 'necessary' for compliance?
- What else should we consider?

What's new?

Very little. The lawful basis for processing necessary for compliance with a legal obligation is almost identical to the old condition for processing in paragraph 3 of Schedule 2 of the 1998 Act.

You need to review your existing processing so that you can document where you rely on this basis and inform individuals. But in practice, if you are confident that your existing approach complied with the 1998 Act, you are unlikely to need to change your existing basis for processing.

What does the GDPR say?

Article 6(1)(c) provides a lawful basis for processing where:

> "processing is necessary for compliance with a legal obligation to which the controller is subject."

When is the lawful basis for legal obligations likely to apply?

In short, when you are obliged to process the personal data to comply with the law.

Article 6(3) requires that the legal obligation must be laid down by UK or EU law. Recital 41 confirms that this does not have to be an explicit statutory obligation, as long as the application of the law is foreseeable to those individuals subject to it. So it includes clear common law obligations.

This does not mean that there must be a legal obligation specifically requiring the specific processing activity. The point is that your overall purpose must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute.

You should be able to identify the obligation in question, either by reference to the specific legal provision or else by pointing to an appropriate source of advice or guidance that sets it out clearly. For example, you can refer to a government website or to industry guidance that explains generally applicable legal obligations.

Example

An employer needs to process personal data to comply with its legal obligation to disclose employee salary details to HMRC.

The employer can point to the HMRC website where the requirements are set out to demonstrate this obligation. In this situation it is not necessary to cite each specific piece of legislation.

Example

A financial institution relies on the legal obligation imposed by the Part 7 of Proceeds of Crime Act 2002 to process personal data in order submit a Suspicious Activity Report to the National Crime Agency when it knows or suspects that a person is engaged in, or attempting, money laundering.

Example

A court order may require you to process personal data for a particular purpose and this also qualifies as a legal obligation.

Regulatory requirements also qualify as a legal obligation for these purposes where there is a statutory basis underpinning the regulatory regime and which requires regulated organisations to comply.

Example

The Competition and Markets Authority (CMA) has powers under The Enterprise Act 2002 to make orders to remedy adverse effects on competition, some of which may require the processing of personal data.

A retail energy supplier passes customer data to the Gas and Electricity Markets Authority to comply with the CMA's Energy Market Investigation (Database) Order 2016. The supplier may rely on legal obligation as the lawful basis for this processing.

A contractual obligation does not comprise a legal obligation in this context. You cannot contract out of the requirement for a lawful basis. However, you can look for a different lawful basis. If the contract is with the individual you can consider the lawful basis for contracts. For contracts with other parties, you may want to consider legitimate interests.

When is processing 'necessary' for compliance?

Although the processing need not be essential for you to comply with the legal obligation, it must be a reasonable and proportionate way of achieving compliance. You cannot rely on this lawful basis if you have discretion over whether to process the personal data, or if there is another reasonable way to comply.

It is likely to be clear from the law in question whether the processing is actually necessary for compliance.

What else should we consider?

If you are processing on the basis of legal obligation, the individual has no right to erasure, right to data portability, or right to object. Read our guidance on individual rights for more information.

Remember to:

- document your decision that processing is necessary for compliance with a legal obligation;
- identify an appropriate source for the obligation in question; and
- include information about your purposes and lawful basis in your privacy notice.

Further Reading

Relevant provisions in the GDPR - See Article 6(1)(c), Recitals 41, 45
External link

In more detail - ICO guidance

We have produced the lawful basis interactive guidance tool, to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

Vital interests

At a glance

- You are likely to be able to rely on vital interests as your lawful basis if you need to process the personal data to protect someone's life.
- The processing must be necessary. If you can reasonably protect the person's vital interests in another less intrusive way, this basis will not apply.
- You cannot rely on vital interests for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.
- You should consider whether you are likely to rely on this basis, and if so document the circumstances where it will be relevant and ensure you can justify your reasoning.

In brief

- What's new?
- What does the GDPR say?
- What are 'vital interests'?
- When is the vital interests basis likely to apply?
- What else should we consider?

What's new?

The lawful basis for vital interests is very similar to the old condition for processing in paragraph 4 of Schedule 2 of the 1998 Act. One key difference is that anyone's vital interests can now provide a basis for processing, not just those of the data subject themselves.

You need to review your existing processing to identify if you have any ongoing processing for this reason, or are likely to need to process for this reason in future. You should then document where you rely on this basis and inform individuals if relevant.

What does the GDPR say?

Article 6(1)(d) provides a lawful basis for processing where:

> "processing is necessary in order to protect the vital interests of the data subject or of another natural person".

Recital 46 provides some further guidance:

> “The processing of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis…”

What are ‘vital interests’?

It’s clear from Recital 46 that vital interests are intended to cover only interests that are essential for someone’s life. So this lawful basis is very limited in its scope, and generally only applies to matters of life and death.

When is the vital interests basis likely to apply?

It is likely to be particularly relevant for emergency medical care, when you need to process personal data for medical purposes but the individual is incapable of giving consent to the processing.

Example

An individual is admitted to the A & E department of a hospital with life-threatening injuries following a serious road accident. The disclosure to the hospital of the individual’s medical history is necessary in order to protect his/her vital interests.

It is less likely to be appropriate for medical care that is planned in advance. Another lawful basis such as public task or legitimate interests is likely to be more appropriate in this case.

Processing of one individual’s personal data to protect the vital interests of others is likely to happen more rarely. It may be relevant, for example, if it is necessary to process a parent’s personal data to protect the vital interests of a child.

Vital interests is also less likely to be the appropriate basis for processing on a larger scale. Recital 46 does suggest that vital interests might apply where you are processing on humanitarian grounds such as monitoring epidemics, or where there is a natural or man-made disaster causing a humanitarian emergency.

However, if you are processing one person’s personal data to protect someone else’s life, Recital 46 also indicates that you should generally try to use an alternative lawful basis, unless none is obviously available. For example, in many cases you could consider legitimate interests, which will give you a framework to balance the rights and interests of the data subject(s) with the vital interests of the person or people you are trying to protect.

What else should we consider?

In most cases the protection of vital interests is likely to arise in the context of health data. This is one of the special categories of data, which means you will also need to identify a condition for processing special category data under Article 9.

There is a specific condition at Article 9(2)(c) for processing special category data where necessary to protect someone's vital interests. However, this only applies if the data subject is physically or legally incapable of giving consent. This means explicit consent is more appropriate in many cases, and you cannot in practice rely on vital interests for special category data (including health data) if the data subject refuses consent, unless they are not competent to do so.

Further Reading

Relevant provisions in the GDPR - See Article 6(1)(d), Article 9(2)(c), Recital 46
External link

In more detail - ICO guidance

We have produced the lawful basis interactive guidance tool, to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

Public task

At a glance

- You can rely on this lawful basis if you need to process personal data:
  - 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or
  - to perform a specific task in the public interest that is set out in law.
- It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.
- You do not need a specific statutory power to process personal data, but your underlying task, function or power must have a clear basis in law.
- The processing must be necessary. If you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply.
- Document your decision to rely on this basis to help you demonstrate compliance if required. You should be able to specify the relevant task, function or power, and identify its statutory or common law basis.

In brief

- What's new under the GDPR?
- What is the 'public task' basis?
- What does 'laid down by law' mean?
- Who can rely on this basis?
- When can we rely on this basis?
- What else should we consider?

What's new under the GDPR?

The public task basis in Article 6(1)(e) may appear new, but it is similar to the old condition for processing for functions of a public nature in Schedule 2 of the Data Protection Act 1998.

One key difference is that the GDPR says that the relevant task or function must have a clear basis in law.

The GDPR is also clear that public authorities can no longer rely on legitimate interests for processing carried out in performance of their tasks. In the past, some of this type of processing may have been done on the basis of legitimate interests. If you are a public authority, this means you may now need to consider the public task basis for more of your processing.

The GDPR also brings in new accountability requirements. You should document your lawful basis so that you can demonstrate that it applies. In particular, you should be able to identify a clear basis in either statute or common law for the relevant task, function or power for which you are using the personal

data.

You must also update your privacy notice to include your lawful basis, and communicate this to individuals.

What is the 'public task' basis?

Article 6(1)(e) gives you a lawful basis for processing where:

> "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"

This can apply if you are either:

- carrying out a specific task in the public interest which is laid down by law; or
- exercising official authority (for example, a public body's tasks, functions, duties or powers) which is laid down by law.

If you can show you are exercising official authority, including use of discretionary powers, there is no additional public interest test. However, you must be able to demonstrate that the processing is 'necessary' for that purpose.

'Necessary' means that the processing must be a targeted and proportionate way of achieving your purpose. You do not have a lawful basis for processing if there is another reasonable and less intrusive way to achieve the same result.

In this guide we use the term 'public task' to help describe and label this lawful basis. However, this is not a term used in the GDPR itself. Your focus should be on demonstrating either that you are carrying out a task in the public interest, or that you are exercising official authority.

In particular, there is no direct link to the concept of 'public task' in the Re-use of Public Sector Information Regulations 2015 (RPSI). There is some overlap, as a public sector body's core role and functions for RPSI purposes may be a useful starting point in demonstrating official authority for these purposes. However, you shouldn't assume that it is an identical test. See our Guide to RPSI for more on public task in the context of RPSI.

What does 'laid down by law' mean?

Article 6(3) requires that the relevant task or authority must be laid down by domestic or EU law. This will most often be a statutory function. However, Recital 41 clarifies that this does not have to be an explicit statutory provision, as long as the application of the law is clear and foreseeable. This means that it includes clear common law tasks, functions or powers as well as those set out in statute or statutory guidance.

You do not need specific legal authority for the particular processing activity. The point is that your overall purpose must be to perform a public interest task or exercise official authority, and that overall

task or authority has a sufficiently clear basis in law.

Who can rely on this basis?

Any organisation who is exercising official authority or carrying out a specific task in the public interest. The focus is on the nature of the function, not the nature of the organisation.

Example

Private water companies are likely to be able to rely on the public task basis even if they do not fall within the definition of a public authority in the Data Protection Bill. This is because they are considered to be carrying out functions of public administration and they exercise special legal powers to carry out utility services in the public interest. See our guidance on Public authorities under the EIR for more details.

However, if you are a private sector organisation you are likely to be able to consider the legitimate interests basis as an alternative.

See the main lawful basis page of this guide for more on how to choose the most appropriate basis.

When can we rely on this basis?

The Data Protection Bill includes a draft clause clarifying that the public task basis will cover processing necessary for:

- the administration of justice;
- parliamentary functions;
- statutory functions; or
- governmental functions.

However, this is not intended as an exhaustive list. If you have other official non-statutory functions or public interest tasks you can still rely on the public task basis, as long as the underlying legal basis for that function or task is clear and foreseeable.

For accountability purposes, you should be able to specify the relevant task, function or power, and identify its basis in common law or statute. You should also ensure that you can demonstrate there is no other reasonable and less intrusive means to achieve your purpose.

What else should we consider?

Individuals' rights to erasure and data portability do not apply if you are processing on the basis of public task. However, individuals do have a right to object. See our guidance on individual rights for more information.

You should consider an alternative lawful basis if you are not confident that processing is necessary for a relevant task, function or power which is clearly set out in law.

If you are a public authority (as defined in the Data Protection Bill), your ability to rely on consent or legitimate interests as an alternative basis is more limited, but they may be available in some circumstances. In particular, legitimate interests is still available for processing which falls outside your tasks as a public authority. Other lawful bases may also be relevant. See our guidance on the other lawful bases for more information. We will publish more guidance on the definition of a public authority when the relevant Bill provisions are finalised.

Remember that the GDPR specifically says that further processing for certain purposes should be considered to be compatible with your original purpose. This means that if you originally processed the personal data for a relevant task or function, you do not need a separate lawful basis for any further processing for:

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

If you are processing special category data, you also need to identify an additional condition for processing this type of data. Read our guidance on special category data for more information. The Data Protection Bill includes specific draft conditions for parliamentary, statutory or governmental functions in the substantial public interest – more guidance on this and other conditions will follow when the Bill is finalised.

To help you meet your accountability and transparency obligations, remember to:

- document your decision that the processing is necessary for you to perform a task in the public interest or exercise your official authority;
- identify the relevant task or authority and its basis in common law or statute; and
- include basic information about your purposes and lawful basis in your privacy notice.

Further Reading

Relevant provisions in the GDPR - See Article 6(1)(e) and 6(3), and Recitals 41, 45 and 50
External link

Relevant provisions in the Data Protection Bill - See clause 8 and Schedule 1 para 6 and 7
External link

In more detail – ICO guidance

We are planning to develop more detailed guidance on this topic.

We have produced the lawful basis interactive guidance tool, to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

Legitimate interests

At a glance

- Legitimate interests is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate.
- It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
- If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.
- Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.
- There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to:
  - identify a legitimate interest;
  - show that the processing is necessary to achieve it; and
  - balance it against the individual's interests, rights and freedoms.
- The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.
- The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.
- You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.
- Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance if required.
- You must include details of your legitimate interests in your privacy information.

Checklists

☐ We have checked that legitimate interests is the most appropriate basis.

☐ We understand our responsibility to protect the individual's interests.

☐ We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.

☐ We have identified the relevant legitimate interests.

☐ We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.

☐ We have done a balancing test, and are confident that the individual's interests do not override those legitimate interests.

☐ We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.

☐ We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.

☐ If we process children's data, we take extra care to make sure we protect their interests.

☐ We have considered safeguards to reduce the impact where possible.

☐ We have considered whether we can offer an opt out.

☐ If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.

☐ We keep our LIA under review, and repeat it if circumstances change.

☐ We include information about our legitimate interests in our privacy information.

In brief

- What's new under the GDPR?
- What is the 'legitimate interests' basis?
- When can we rely on legitimate interests?
- How can we apply legitimate interests in practice?
- What else do we need to consider?

What's new under the GDPR?

The concept of legitimate interests as a lawful basis for processing is essentially the same as the equivalent Schedule 2 condition in the 1998 Act, with some changes in detail.

You can now consider the legitimate interests of any third party, including wider benefits to society. And when weighing against the individual's interests, the focus is wider than the emphasis on 'unwarranted prejudice' to the individual in the 1998 Act. For example, unexpected processing is likely to affect whether the individual's interests override your legitimate interests, even without specific harm.

The GDPR is clearer that you must give particular weight to protecting children's data.

Public authorities are more limited in their ability to rely on legitimate interests, and should consider the 'public task' basis instead for any processing they do to perform their tasks as a public authority. Legitimate interests may still be available for other legitimate processing outside of those tasks.

The biggest change is that you need to document your decisions on legitimate interests so that you can demonstrate compliance under the new GDPR accountability principle. You must also include more information in your privacy information.

In the run up to 25 May 2018, you need to review your existing processing to identify your lawful basis and document where you rely on legitimate interests, update your privacy information, and communicate it to individuals.

What is the 'legitimate interests' basis?

Article 6(1)(f) gives you a lawful basis for processing where:

> "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

This can be broken down into a three-part test:

1. **Purpose test:** are you pursuing a legitimate interest?
2. **Necessity test:** is the processing necessary for that purpose?
3. **Balancing test:** do the individual's interests override the legitimate interest?

A wide range of interests may be legitimate interests. They can be your own interests or the interests of third parties, and commercial interests as well as wider societal benefits. They may be compelling or trivial, but trivial interests may be more easily overridden in the balancing test.

The GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list. It also says that you have a legitimate interest in disclosing information about possible criminal acts or security threats to the authorities.

'Necessary' means that the processing must be a targeted and proportionate way of achieving your purpose. You cannot rely on legitimate interests if there is another reasonable and less intrusive way to achieve the same result.

You must balance your interests against the individual's interests. In particular, if they would not reasonably expect you to use data in that way, or it would cause them unwarranted harm, their interests are likely to override yours. However, your interests do not always have to align with the individual's interests. If there is a conflict, your interests can still prevail as long as there is a clear justification for the impact on the individual.

When can we rely on legitimate interests?

Legitimate interests is the most flexible lawful basis, but you cannot assume it will always be appropriate for all of your processing.

If you choose to rely on legitimate interests, you take on extra responsibility for ensuring people's rights and interests are fully considered and protected.

Legitimate interests is most likely to be an appropriate basis where you use data in ways that people

would reasonably expect and that have a minimal privacy impact. Where there is an impact on individuals, it may still apply if you can show there is an even more compelling benefit to the processing and the impact is justified.

You can rely on legitimate interests for marketing activities if you can show that how you use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object – but only if you don't need consent under PECR. See our Guide to PECR for more on when you need consent for electronic marketing.

You can consider legitimate interests for processing children's data, but you must take extra care to make sure their interests are protected. See our detailed guidance on children and the GDPR.

You may be able to rely on legitimate interests in order to lawfully disclose personal data to a third party. You should consider why they want the information, whether they actually need it, and what they will do with it. You need to demonstrate that the disclosure is justified, but it will be their responsibility to determine their lawful basis for their own processing.

You should avoid using legitimate interests if you are using personal data in ways people do not understand and would not reasonably expect, or if you think some people would object if you explained it to them. You should also avoid this basis for processing that could cause harm, unless you are confident there is nevertheless a compelling reason to go ahead which justifies the impact.

If you are a public authority, you cannot rely on legitimate interests for any processing you do to perform your tasks as a public authority. However, if you have other legitimate purposes outside the scope of your tasks as a public authority, you can consider legitimate interests where appropriate. This will be particularly relevant for public authorities with commercial interests.

See our guidance page on the lawful basis for more information on the alternatives to legitimate interests, and how to decide which basis to choose.

How can we apply legitimate interests in practice?

If you want to rely on legitimate interests, you can use the three-part test to assess whether it applies. We refer to this as a legitimate interests assessment (LIA) and you should do it before you start the processing.

An LIA is a type of light-touch risk assessment based on the specific context and circumstances. It will help you ensure that your processing is lawful. Recording your LIA will also help you demonstrate compliance in line with your accountability obligations under Articles 5(2) and 24. In some cases an LIA will be quite short, but in others there will be more to consider.

First, identify the legitimate interest(s). Consider:

- Why do you want to process the data – what are you trying to achieve?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if you couldn't go ahead?
- Would your use of the data be unethical or unlawful in any way?

Second, apply the necessity test. Consider:

- Does this processing actually help to further that interest?
- Is it a reasonable way to go about it?
- Is there another less intrusive way to achieve the same result?

Third, do a balancing test. Consider the impact of your processing and whether this overrides the interest you have identified. You might find it helpful to think about the following:

- What is the nature of your relationship with the individual?
- Is any of the data particularly sensitive or private?
- Would people expect you to use their data in this way?
- Are you happy to explain it to them?
- Are some people likely to object or find it intrusive?
- What is the possible impact on the individual?
- How big an impact might it have on them?
- Are you processing children's data?
- Are any of the individuals vulnerable in any other way?
- Can you adopt any safeguards to minimise the impact?
- Can you offer an opt-out?

You then need to make a decision about whether you still think legitimate interests is an appropriate basis. There's no foolproof formula for the outcome of the balancing test – but you must be confident that your legitimate interests are not overridden by the risks you have identified.

Keep a record of your LIA and the outcome. There is no standard format for this, but it's important to record your thinking to help show you have proper decision-making processes in place and to justify the outcome.

Keep your LIA under review and refresh it if there is a significant change in the purpose, nature or context of the processing.

If you are not sure about the outcome of the balancing test, it may be safer to look for another lawful basis. Legitimate interests will not often be the most appropriate basis for processing which is unexpected or high risk.

If your LIA identifies significant risks, consider whether you need to do a DPIA to assess the risk and potential mitigation in more detail. See our guidance on DPIAs for more on this.

What else do we need to consider?

You must tell people in your privacy information that you are relying on legitimate interests, and explain what these interests are.

If you want to process the personal data for a new purpose, you may be able to continue processing under legitimate interests as long as your new purpose is compatible with your original purpose. We would still recommend that you conduct a new LIA, as this will help you demonstrate compatibility.

If you rely on legitimate interests, the right to data portability does not apply.

If you are relying on legitimate interests for direct marketing, the right to object is absolute and you must stop processing when someone objects. For other purposes, you must stop unless you can show that your legitimate interests are compelling enough to override the individual's rights. See our guidance on individual rights for more on this.

Further Reading

Relevant provisions in the GDPR - See Article 6(1)(f) and Recitals 47, 48 and 49
External link

In more detail – ICO guidance

We have produced more detailed guidance on legitimate interests

We have produced the lawful basis interactive guidance tool, to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

In more detail - Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

There are no immediate plans for Article 29 Working Party guidance on legitimate interests under the GDPR, but WP29 Opinion 06/2014 (9 April 2014) gives detailed guidance on the key elements of the similar legitimate interests provisions under the previous Data Protection Directive 95/46/EC.

Special category data

At a glance

- Special category data is personal data which the GDPR says is more sensitive, and so needs more protection.
- In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These do not have to be linked.
- There are ten conditions for processing special category data in the GDPR itself, but the Data Protection Bill will introduce additional conditions and safeguards.
- You must determine your condition for processing special category data before you begin this processing under the GDPR, and you should document it.

In brief

- What's new?
- What's different about special category data?
- What are the conditions for processing special category data?

What's new?

Special category data is broadly similar to the concept of sensitive personal data under the 1998 Act. The requirement to identify a specific condition for processing this type of data is also very similar.

One change is that the GDPR includes genetic data and some biometric data in the definition. Another is that it does not include personal data relating to criminal offences and convictions, as there are separate and specific safeguards for this type of data in Article 10. See the definitions section of this Guide for more detail on what counts as special category data.

The conditions for processing special category data under the GDPR in the UK are likely to be similar to the Schedule 3 conditions under the 1998 Act for the processing of sensitive personal data. More detailed guidance on the special category conditions and how they differ from existing Schedule 3 conditions will follow as the Data Protection Bill is finalised.

What’s different about special category data?

You must still have a lawful basis for your processing under Article 6, in exactly the same way as for any other personal data. The difference is that you will also need to satisfy a specific condition under Article 9.

This is because special category data is more sensitive, and so needs more protection. For example, information about an individual’s:

- race;

- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

See the definitions section of this Guide for full details.

In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

Your choice of lawful basis under Article 6 does not dictate which special category condition you must apply, and vice versa. For example, if you use consent as your lawful basis, you are not restricted to using explicit consent for special category processing under Article 9. You should choose whichever special category condition is the most appropriate in the circumstances – although in many cases there may well be an obvious link between the two. For example, if your lawful basis is vital interests, it is highly likely that the Article 9 condition for vital interests will also be appropriate.

What are the conditions for processing special category data?

The conditions are listed in Article 9(2) of the GDPR:

> (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
>
> (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
>
> (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
>
> (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Some of these conditions make reference to UK law, and the GDPR also gives member states the scope to add more conditions. The Data Protection Bill includes proposals for additional conditions and safeguards, and we will publish more detailed guidance here once these provisions are finalised.

Further Reading

Relevant provisions in the GDPR - See Article 9(2) and Recital 51
External link

Relevant provisions in the Data Protection Bill - See clauses 9 and 10, and Schedule 1
External link

Criminal offence data

At a glance

- To process personal data about criminal convictions or offences, you must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10.
- The Data Protection Bill deals with this type of data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it.
- You can also process this type of data if you have official authority to do so because you are processing the data in an official capacity.
- You cannot keep a comprehensive register of criminal convictions unless you do so in an official capacity.
- You must determine your condition for lawful processing of offence data (or identify your official authority for the processing) before you begin the processing, and you should document this.

In brief

- What's new?
- What is criminal offence data?
- What's different about criminal offence data?
- What are the conditions for processing criminal offence data?

What's new?

The GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures, set out in Article 10.

Article 10 also specifies that you can only keep a comprehensive register of criminal convictions if you are doing so under the control of official authority.

What is criminal offence data?

Article 10 applies to personal data relating to criminal convictions and offences, or related security measures. In this guidance, we refer to this as criminal offence data.

This concept of criminal offence data includes the type of data about criminal allegations, proceedings or convictions that would have been sensitive personal data under the 1998 Act. However, it is potentially broader than this. In particular, Article 10 specifically extends to personal data linked to related security measures.

What's different about criminal offence data?

You must still have a lawful basis for your processing under Article 6, in exactly the same way as for any other personal data. The difference is that if you are processing personal criminal offence data, you will

also need to comply with Article 10.

What does Article 10 say?

Article 10 says:

> "Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority."

This means you must either be processing the data in an official capacity, or have specific legal authorisation – which in the UK, is likely to mean a condition under the Data Protection Bill and compliance with the additional safeguards set out in the Bill. We will publish more detailed guidance on the conditions in the Bill once these provisions are finalised.

Even if you have a condition for processing offence data, you can only keep a comprehensive register of criminal convictions if you are doing so in an official capacity.

Further Reading

Relevant provisions in the GDPR - see Article 10
External link

Relevant provisions in the Data Protection Bill - See clauses 9 and 10, and Schedule 1
External link

Individual rights

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

This part of the guide explains these rights.

Right to be informed

At a glance

- Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.
- You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with. We call this 'privacy information'.
- You must provide privacy information to individuals at the time you collect their personal data from them.
- If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.
- There are a few circumstances when you do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.
- The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.
- It is often most effective to provide privacy information to people using a combination of different techniques including layering, dashboards, and just-in-time notices.
- User testing is a good way to get feedback on how effective the delivery of your privacy information is.
- You must regularly review, and where necessary, update your privacy information. You must bring any new uses of an individual's personal data to their attention before you start the processing.
- Getting the right to be informed correct can help you to comply with other aspects of the GDPR and build trust with people, but getting it wrong can leave you open to fines and lead to reputational damage.

Checklists

What to provide

We provide individuals with all the following privacy information:

☐ The name and contact details of our organisation.

☐ The name and contact details of our representative (if applicable).

☐ The contact details of our data protection officer (if applicable).

☐ The purposes of the processing.

☐ The lawful basis for the processing.

☐ The legitimate interests for the processing (if applicable).

☐ The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).

☐ The recipients or categories of recipients of the personal data.

☐ The details of transfers of the personal data to any third countries or international organisations (if applicable).

☐ The retention periods for the personal data.

☐ The rights available to individuals in respect of the processing.

☐ The right to withdraw consent (if applicable).

☐ The right to lodge a complaint with a supervisory authority.

☐ The source of the personal data (if the personal data is not obtained from the individual it relates to).

☐ The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).

☐ The details of the existence of automated decision-making, including profiling (if applicable).

When to provide it

☐ We provide individuals with privacy information at the time we collect their personal data from them.

If we obtain personal data from a source other than the individual it relates to, we provide them with privacy information:

- ☐ within a reasonable of period of obtaining the personal data and no later than one month;
- ☐ if we plan to communicate with the individual, at the latest, when the first communication takes place; or
- ☐ if we plan to disclose the data to someone else, at the latest, when the data is disclosed.

How to provide it

We provide the information in a way that is:

- ☐ concise;
- ☐ transparent;
- ☐ intelligible;
- ☐ easily accessible; and

☐ uses clear and plain language.

Changes to the information

☐ We regularly review and, where necessary, update our privacy information.

☐ If we plan to use personal data for a new purpose, we update our privacy information and communicate the changes to individuals before starting any new processing.

Best practice – drafting the information

☐ We undertake an information audit to find out what personal data we hold and what we do with it.

☐ We put ourselves in the position of the people we're collecting information about.

☐ We carry out user testing to evaluate how effective our privacy information is.

Best practice – delivering the information

When providing our privacy information to individuals, we use a combination of appropriate techniques, such as:

☐ a layered approach;

☐ dashboards;

☐ just-in-time notices;

☐ icons; and

☐ mobile and smart device functionalities.

In brief

- What's new under the GDPR?
- What is the right to be informed and why is it important?
- What privacy information should we provide to individuals?
- When should we provide privacy information to individuals?
- How should we draft our privacy information?
- How should we provide privacy information to individuals?
- Should we test, review and update our privacy information?

What's new under the GDPR?

The GDPR is more specific about the information you need to provide to people about what you do with their personal data.

You must actively provide this information to individuals in a way that is easy to access, read and understand.

You should review your current approach for providing privacy information to check it meets the standards of the GDPR.

What is the right to be informed and why is it important?

The right to be informed covers some of the key transparency requirements of the GDPR. It is about providing people with clear and concise information about what you do with their personal data.

Articles 13 and 14 of the GDPR specify what individuals have the right to be informed about. We call this 'privacy information'.

Using an effective approach to provide people with privacy information can help you to comply with other aspects of the GDPR, foster trust with individuals and obtain more useful information from them.

Getting this wrong can leave you open to fines and lead to reputational damage.

What privacy information should we provide to individuals?

The table below summarises the information that you must provide. What you need to tell people differs slightly depending on whether you collect personal data from the individual it relates to or obtain it from another source.

What information do we need to provide?	**Personal data collected from individuals**	**Personal data obtained from other sources**
The name and contact details of your organisation	✓	✓
The name and contact details of your representative	✓	✓
The contact details of your data protection officer	✓	✓
The purposes of the processing	✓	✓
The lawful basis for the processing	✓	✓
The legitimate interests for the processing	✓	✓
The categories of personal data obtained		✓
The recipients or categories of recipients of the personal data	✓	✓
The details of transfers of the personal data to any third countries or international organisations	✓	✓

The retention periods for the personal data	✓	✓
The rights available to individuals in respect of the processing	✓	✓
The right to withdraw consent	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source of the personal data		✓
The details of whether individuals are under a statutory or contractual obligation to provide the personal data	✓	
The details of the existence of automated decision-making, including profiling	✓	✓

When should we provide privacy information to individuals?

When you collect personal data from the individual it relates to, you must provide them with privacy information at the time you obtain their data.

When you obtain personal data from a source other than the individual it relates to, you need to provide the individual with privacy information:

- within a reasonable of period of obtaining the personal data and no later than one month;
- if the data is used to communicate with the individual, at the latest, when the first communication takes place; or
- if disclosure to someone else is envisaged, at the latest, when the data is disclosed.

You must actively provide privacy information to individuals. You can meet this requirement by putting the information on your website, but you must make individuals aware of it and give them an easy way to access it.

When collecting personal data from individuals, you do not need to provide them with any information that they already have.

When obtaining personal data from other sources, you do not need to provide individuals with privacy information if:

- the individual already has the information;
- providing the information to the individual would be impossible;
- providing the information to the individual would involve a disproportionate effort;
- providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing;
- you are required by law to obtain or disclose the personal data; or
- you are subject to an obligation of professional secrecy regulated by law that covers the personal data.

How should we draft our privacy information?

An information audit or data mapping exercise can help you find out what personal data you hold and what you do with it.

You should think about the intended audience for your privacy information and put yourself in their position.

If you collect or obtain children's personal data, you must take particular care to ensure that the information you provide them with is appropriately written, using clear and plain language.

For all audiences, you must provide information to them in a way that is:

- concise;
- transparent;
- intelligible;
- easily accessible; and
- uses clear and plain language.

How should we provide privacy information to individuals?

There are a number of techniques you can use to provide people with privacy information. You can use:

- **A layered approach** – short notices containing key privacy information that have additional layers of more detailed information.
- **Dashboards** – preference management tools that inform people how their data is used and allow them to manage what happens with it.
- **Just-in-time notices** – relevant and focused privacy information delivered at the time individual pieces of information about people are collected.
- **Icons** – small, meaningful, symbols that indicate the existence of a particular type of data processing.
- **Mobile and smart device functionalities** – including pop-ups, voice alerts and mobile device gestures.

Consider the context in which you are collecting personal data. It is good practice to use the same medium you use to collect personal data to deliver privacy information.

Taking a blended approach, using more than one of these techniques, is often the most effective way to provide privacy information.

Should we test, review and update our privacy information?

It is good practice to carry out user testing on your draft privacy information to get feedback on how easy it is to access and understand.

After it is finalised, undertake regular reviews to check it remains accurate and up to date.

If you plan to use personal data for any new purposes, you must update your privacy information and proactively bring any changes to people's attention.

Further Reading

Relevant provisions in the GDPR – See Articles 12-14, and Recitals 58 and 60-62
External link

In more detail – ICO guidance

We are planning to publish more detailed guidance on this topic shortly, taking account of the Article 29 Working Party guidelines which are currently being finalised.

In more detail – Article 29

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 has published draft guidelines on Transparency. These were subject to a consultation process and the final version is due to be adopted in April 2018.

Right of access

At a glance

- Individuals have the right to access their personal data and supplementary information.
- The right of access allows individuals to be aware of and verify the lawfulness of the processing.

In brief

What information is an individual entitled to under the GDPR?

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

What is the purpose of the right of access under GDPR?

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (Recital 63).

Can I charge a fee for dealing with a subject access request?

You must provide a copy of the information **free of charge**. However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information.

How long do I have to comply?

Information must be provided without delay and at the latest within one month of receipt.

You will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

What if the request is manifestly unfounded or excessive?

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

Where you refuse to respond to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

How should the information be provided?

You must verify the identity of the person making the request, using 'reasonable means'.

If the request is made electronically, you should provide the information in a commonly used electronic format.

The GDPR includes a best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information (Recital 63). This will not be appropriate for all organisations, but there are some sectors where this may work well.

The right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others.

What about requests for large amounts of personal data?

Where you process a large quantity of information about an individual, the GDPR permits you to ask the individual to specify the information the request relates to (Recital 63).

The GDPR does not include an exemption for requests that relate to large amounts of data, but you may be able to consider whether the request is manifestly unfounded or excessive.

Further Reading

Relevant provisions in the GDPR - see Articles 12 and 15 and Recital 63
External link

Right to rectification

At a glance

- The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- You have one calendar month to respond to a request.
- In certain circumstances you can refuse a request for rectification.
- This right is closely linked to the controller's obligations under the accuracy principle of the GDPR (Article (5)(1)(d)).

Checklists

Preparing for requests for rectification

☐ We know how to recognise a request for rectification and we understand when this right applies.

☐ We have a policy for how to record requests we receive verbally.

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for rectification

☐ We have processes in place to ensure that we respond to a request for rectification without undue delay and within one month of receipt.

☐ We are aware of the circumstances when we can extend the time limit to respond to a request.

☐ We have appropriate systems to rectify or complete information, or provide a supplementary statement.

☐ We have procedures in place to inform any recipients if we rectify any data we have shared with them.

In brief

What is the right to rectification?

Under Article 16 of the GDPR individuals have the right to have inaccurate personal data rectified. An

individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

This right has close links to the accuracy principle of the GDPR (Article 5(1)(d)). However, although you may have already taken steps to ensure that the personal data was accurate when you obtained it, this right imposes a specific obligation to reconsider the accuracy upon request.

What do we need to do?

If you receive a request for rectification you should take reasonable steps to satisfy yourself that the data is accurate and to rectify the data if necessary. You should take into account the arguments and evidence provided by the data subject.

What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort you should put into checking its accuracy and, if necessary, taking steps to rectify it. For example, you should make a greater effort to rectify inaccurate personal data if it is used to make significant decisions that will affect an individual or others, rather than trivial ones.

You may also take into account any steps you have already taken to verify the accuracy of the data prior to the challenge by the data subject.

When is data inaccurate?

The GDPR does not give a definition of the term accuracy. However, the Data Protection Bill states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

What should we do about data that records a mistake?

Determining whether personal data is inaccurate can be more complex if the data refers to a mistake that has subsequently been resolved. It may be possible to argue that the record of the mistake is, in itself, accurate and should be kept. In such circumstances the fact that a mistake was made and the correct information should also be included in the individuals data.

Example

If a patient is diagnosed by a GP as suffering from a particular illness or condition, but it is later proved that this is not the case, it is likely that their medical records should record both the initial diagnosis (even though it was later proved to be incorrect) and the final findings. Whilst the medical record shows a misdiagnosis, it is an accurate record of the patient's medical treatment. As long as the medical record contains the up-to-date findings, and this is made clear in the record, it would be difficult to argue that the record is inaccurate and should be rectified.

What should we do about data that records a disputed opinion?

It is also complex if the data in question records an opinion. Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified.

What should we do while we are considering the accuracy?

Under Article 18 an individual has the right to request restriction of the processing of their personal data where they contest its accuracy and you are checking it. As a matter of good practice, you should restrict the processing of the personal data in question whilst you are verifying its accuracy, whether or not the individual has exercised their right to restriction. For more information, see our guidance on the right to restriction.

What should we do if we are satisfied that the data is accurate?

You should let the individual know if you are satisfied that the personal data is accurate, and tell them that you will not be amending the data. You should explain your decision, and inform them of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy.

It is also good practice to place a note on your system indicating that the individual challenges the accuracy of the data and their reasons for doing so.

Can we refuse to comply with the request for rectification for other reasons?

You can refuse to comply with a request for rectification if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If you consider that a request is manifestly unfounded or excessive you can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case you will need to justify your decision.

You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual without undue delay and within one month. You do not need to comply with the request until you have received the fee.

In more detail – Data Protection Bill

There are other proposed exemptions from the right to rectification that are contained in the draft DP Bill. As proposed, these exemptions will apply in certain circumstances, broadly associated with why you are processing the data. Once the DP Bill is finalised, we will update our guidance accordingly, and provide further detail on the application of these exemptions.

What should we do if we refuse to comply with a request for rectification?

You must inform the individual without undue delay and within one month of receipt of the request about:

- the reasons you are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

How can we recognise a request?

The GDPR does not specify how to make a valid request. Therefore, an individual can make a request for rectification verbally or in writing. It can also be made to any part of your organisation and does not have to be to a specific person or contact point.

A request to rectify personal data does not need to mention the phrase 'request for rectification' or Article 16 of the GDPR to be a valid request. As long as the individual has challenged the accuracy of their data and has asked you to correct it, or has asked that you take steps to complete data held about them that is incomplete, this will be a valid request under Article 16.

This presents a challenge as any of your employees could receive a valid verbal request. However, you have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore you may need to consider which of your staff who regularly interact with individuals may need specific training to identify a request.

Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request. We also recommend that you keep a log of verbal requests.

Can we charge a fee?

No, in most cases you cannot charge a fee to comply with a request for rectification.

However, as noted above, if the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.

How long do we have to comply?

You must act upon the request without undue delay and at the latest within one month of receipt.

You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

Example

An organisation receives a request on 3 September. The time limit will start from the next day (4

September). This gives the organisation until 4 October to comply with the request.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.

If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

Example

An organisation receives a request on 30 March. The time limit starts from the next day (31 March). As there is no equivalent date in April, the organisation has until 30 April to comply with the request.

If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.

For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Can we extend the time to respond to a request?

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know without undue delay and within one month of receiving their request and explain why the extension is necessary.

The circumstances in which you can extend the time to respond can include further consideration of the accuracy of disputed data - although you can only do this in complex cases - and the result may be that at the end of the extended time period you inform the individual that you consider the data in question to be accurate.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- you are requesting proof of identity before considering the request.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

You must let the individual know without undue delay and within one month that you need more information from them to confirm their identity. You do not need to comply with the request until you have received the additional information.

Do we have to tell other organisations if we rectify personal data?

If you have disclosed the personal data to others, you must contact each recipient and inform them of the rectification or completion of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individual about these recipients.

The GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Further Reading

Relevant provisions in the GDPR - See Articles 5, 12, 16 and 19
External link

Right to erasure

At a glance

- The GDPR introduces a right for individuals to have personal data erased.
- The right to erasure is also known as 'the right to be forgotten'.
- Individuals can make a request for erasure verbally or in writing.
- You have one month to respond to a request.
- The right is not absolute and only applies in certain circumstances.
- This right is not the only way in which the GDPR places an obligation on you to consider whether to delete personal data.

Checklists

Preparing for requests for erasure

☐ We know how to recognise a request for erasure and we understand when the right applies.

☐ We have a policy for how to record requests we receive verbally.

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for erasure

☐ We have processes in place to ensure that we respond to a request for erasure without undue delay and within one month of receipt.

☐ We are aware of the circumstances when we can extend the time limit to respond to a request.

☐ We understand that there is a particular emphasis on the right to erasure if the request relates to data collected from children.

☐ We have procedures in place to inform any recipients if we erase any data we have shared with them.

☐ We have appropriate methods in place to erase information.

In brief

What is the right to erasure?

Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

When does the right to erasure apply?

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

How does the right to erasure apply to data collected from children?

There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the GDPR.

Therefore, if you process data collected from children, you should give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet. This is still the case when the data subject is no longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent.

For further details about the right to erasure and children's personal data please read our guidance on children's privacy.

Do we have to tell other organisations about the erasure of personal data?

The GDPR specifies two circumstances where you should tell other organisations about the erasure of personal data:

- the personal data has been disclosed to others; or
- the personal data has been made public in an online environment (for example on social networks, forums or websites).

If you have disclosed the personal data to others, you must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individuals about these recipients.

The GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Where personal data has been made public in an online environment reasonable steps should be taken to inform other controllers who are processing the personal data to erase links to, copies or replication of that data. When deciding what steps are reasonable you should take into account available technology and the cost of implementation.

When does the right to erasure not apply?

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

The GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- if the processing is necessary for public health purposes in the public interest (eg protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- if the processing is necessary for the purposes of preventative or occupational medicine (eg where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).

For more information about special categories of data please see our Guide to the GDPR.

Can we refuse to comply with a request for other reasons?

You can refuse to comply with a request for erasure if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If you consider that a request is manifestly unfounded or excessive you can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case you will need to justify your decision.

You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

In more detail – Data Protection Bill

There are other proposed exemptions from the right to erasure that are contained in the draft DP Bill. As proposed, these exemptions will apply in certain circumstances, broadly associated with why you are processing the data. Once the DP Bill is finalised, we will update our guidance accordingly, and provide further detail on the application of these exemptions.

What should we do if we refuse to comply with a request for erasure?

You must inform the individual without undue delay and within one month of receipt of the request.

You should inform the individual about:

- the reasons you are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

How do we recognise a request?

The GDPR does not specify how to make a valid request. Therefore, an individual can make a request for erasure verbally or in writing. It can also be made to any part of your organisation and does not have to be to a specific person or contact point.

A request does not have to include the phrase 'request for erasure' or Article 17 of the GDPR, as long as one of the conditions listed above apply.

This presents a challenge as any of your employees could receive a valid verbal request. However, you have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore you may need to consider which of your staff who regularly interact with individuals may need specific training to identify a request.

Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request. We also recommend that you keep a log of verbal requests.

Can we charge a fee?

No, in most cases you cannot charge a fee to comply with a request for erasure.

However, as noted above, where the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.

How long do we have to comply?

You must act upon the request without undue delay and at the latest within one month of receipt.

You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

Example

An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 4 October to comply with the request.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.

If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

This means that the exact number of days you have to comply with a request varies, depending on the month in which the request is made.

Example

An organisation receives a request on 30 March. The time limit starts from the next day (31 March). As there is no equivalent date in April, the organisation has until 30 April to comply with the request.

If 30 April falls on a weekend or is a public holiday, the organisation has until the end of the next working day to comply.

For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Can we extend the time for a response?

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know without undue delay and within one month of receiving their request and explain why the extension is necessary.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- you are requesting proof of identity before considering the request.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

You must let the individual know without undue delay and within one month that you need more information from them to confirm their identity. You do not need to comply with the request until you have received the additional information.

Further Reading

Relevant provisions in the GDPR - See Articles 6, 9, 12, 17 and Recitals 65, 66
External link

Right to restrict processing

At a glance

- Individuals have the right to request the restriction or suppression of their personal data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, you are permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- You have one calendar month to respond to a request.
- This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

Checklists

Preparing for requests for restriction

☐ We know how to recognise a request for restriction and we understand when the right applies.

☐ We have a policy in place for how to record requests we receive verbally.

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for restriction

☐ We have processes in place to ensure that we respond to a request for restriction without undue delay and within one month of receipt.

☐ We are aware of the circumstances when we can extend the time limit to respond to a request.

☐ We have appropriate methods in place to restrict the processing of personal data on our systems.

☐ We have appropriate methods in place to indicate on our systems that further processing has been restricted.

☐ We understand the circumstances when we can process personal data that has been restricted.

☐ We have procedures in place to inform any recipients if we restrict any data we have shared with them.

☐ We understand that we need to tell individuals before we lift a restriction on processing.

In brief

What is the right to restrict processing?

Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how you have processed their data. In most cases you will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time.

When does the right to restrict processing apply?

Individuals have the right to request you restrict the processing of their personal data in the following circumstances:

- the individual contests the accuracy of their personal data and you are verifying the accuracy of the data;
- the data has been unlawfully processed (ie in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- you no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to you processing their data under Article 21(1), and you are considering whether your legitimate grounds override those of the individual.

Although this is distinct from the right to rectification and the right to object, there are close links between those rights and the right to restrict processing:

- if an individual has challenged the accuracy of their data and asked for you to rectify it (Article 16), they also have a right to request you restrict processing while you consider their rectification request; or
- if an individual exercises their right to object under Article 21(1), they also have a right to request you restrict processing while you consider their objection request.

Therefore, as a matter of good practice you should automatically restrict the processing whilst you are considering its accuracy or the legitimate grounds for processing the personal data in question.

How do we restrict processing?

You need to have processes in place that enable you to restrict personal data if required. It is important to note that the definition of processing includes a broad range of operations including collection, structuring, dissemination and erasure of data. Therefore, you should use methods of restriction that are appropriate for the type of processing you are carrying out.

The GDPR suggests a number of different methods that could be used to restrict data, such as:

- temporarily moving the data to another processing system;

- making the data unavailable to users; or
- temporarily removing published data from a website.

It is particularly important that you consider how you store personal data that you no longer need to process but the individual has requested you restrict (effectively requesting that you do not erase the data).

If you are using an automated filing system, you need to use technical measures to ensure that any further processing cannot take place and that the data cannot be changed whilst the restriction is in place. You should also note on your system that the processing of this data has been restricted.

Can we do anything with restricted data?

You must not process the restricted data in any way **except to store it** unless:

- you have the individual's consent;
- it is for the establishment, exercise or defence of legal claims;
- it is for the protection of the rights of another person (natural or legal); or
- it is for reasons of important public interest.

Do we have to tell other organisations about the restriction of personal data?

Yes. If you have disclosed the personal data in question to others, you must contact each recipient and inform them of the restriction of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individual about these recipients.

The GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

When can we lift the restriction?

In many cases the restriction of processing is only temporary, specifically when the restriction is on the grounds that:

- the individual has disputed the accuracy of the personal data and you are investigating this; or
- the individual has objected to you processing their data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of your legitimate interests, and you are considering whether your legitimate grounds override those of the individual.

Once you have made a decision on the accuracy of the data, or whether your legitimate grounds override those of the individual, you may decide to lift the restriction.

If you do this, you must inform the individual **before** you lift the restriction.

As noted above, these two conditions are linked to the right to rectification (Article 16) and the right to object (Article 21). This means that if you are informing the individual that you are lifting the restriction (on the grounds that you are satisfied that the data is accurate, or that your legitimate grounds override theirs) you should also inform them of the reasons for your refusal to act upon their rights under Articles 16 or 21. You will also need to inform them of their right to make a complaint to the ICO or another

supervisory authority; and their ability to seek a judicial remedy.

Can we refuse to comply with a request for restriction?

You can refuse to comply with a request for restriction if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If you consider that a request is manifestly unfounded or excessive you can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case you will need to justify your decision.

You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

In more detail – Data Protection Bill

There are other proposed exemptions from the right to restriction that are contained in the draft DP Bill. As proposed, these exemptions will apply in certain circumstances, broadly associated with why you are processing the data. Once the DP Bill is finalised, we will update our guidance accordingly, and provide further detail on the application of these exemptions.

What should we do if we refuse to comply with a request for restriction?

You must inform the individual without undue delay and within one month of receipt of the request.

You should inform the individual about:

- the reasons you are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

How do we recognise a request?

The GDPR does not specify how to make a valid request. Therefore, an individual can make a request for restriction verbally or in writing. It can also be made to any part of your organisation and does not have to be to a specific person or contact point.

A request does not have to include the phrase 'request for restriction' or Article 18 of the GDPR, as long as one of the conditions listed above apply.

This presents a challenge as any of your employees could receive a valid verbal request. However, you

have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore you may need to consider which of your staff who regularly interact with individuals may need specific training to identify a request.

Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request. We also recommend that you keep a log of verbal requests.

Can we charge a fee?

No, in most cases you cannot charge a fee to comply with a request for restriction.

However, as noted above, where the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.

How long do we have to comply?

You must act upon the request without undue delay and at the latest within one month of receipt.

You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

Example

An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 4 October to comply with the request.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.

If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

Example

An organisation receives a request on 30 March. The time limit starts from the next day (31 March). As there is no equivalent date in April, the organisation has until 30 April to comply with the request.

If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.

For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Can we extend the time for a response?

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- you are requesting proof of identity before considering the request.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

You must let the individual know without undue delay and within one month that you need more information from them to confirm their identity. You do not need to comply with the request until you have received the additional information.

Further Reading

Relevant provisions in the GDPR - See Articles 18, 19 and Recital 67
External link

Right to data portability

At a glance

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.
- The right only applies to information an individual has provided to a controller.
- Some organisations in the UK already offer data portability through midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe.

Checklists

Preparing for requests for data portability

☐ We know how to recognise a request for data portability and we understand when the right applies.

☐ We have a policy for how to record requests we receive verbally.

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for data portability

☐ We can transmit personal data in structured, commonly used and machine readable formats.

☐ We use secure methods to transmit personal data.

☐ We have processes in place to ensure that we respond to a request for data portability without undue delay and within one month of receipt.

☐ We are aware of the circumstances when we can extend the time limit to respond to a request.

In brief

What is the right to data portability?

The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller.

When does the right apply?

The right to data portability only applies when:

- your lawful basis for processing this information is consent **or** for the performance of a contract; and
- you are carrying out the processing by automated means (ie excluding paper files).

What does the right apply to?

Information is only within the scope of the right to data portability if it is personal data of the individual that they have provided to you.

What does 'provided to a controller' mean?

Sometimes the personal data an individual has provided to you will be easy to identify (eg their mailing address, username, age). However, the meaning of data 'provided to' you is not limited to this. It is also personal data resulting from observation of an individual's activities (eg where using a device or service).

This may include:

- history of website usage or search activities;
- traffic and location data; or
- 'raw' data processed by connected objects such as smart meters and wearable devices.

It does not include any additional data that you have created based on the data an individual has provided to you. For example, if you use the data they have provided to create a user profile then this data would not be in scope of data portability.

You should however note that if this 'inferred' or 'derived' data is personal data, you still need to provide it to an individual if they make a subject access request. Bearing this in mind, if it is clear that the individual is seeking access to the inferred/derived data, as part of a wider portability request, it would be good practice to include this data in your response.

Does the right apply to anonymous or pseudonymous data?

The right to data portability only applies to personal data. This means that it does not apply to genuinely anonymous data. However, pseudonymous data that can be clearly linked back to an individual (eg where that individual provides the respective identifier) is within scope of the right.

What happens if the personal data includes information about others?

If the requested information includes information about others (eg third party data) you need to consider whether transmitting that data would adversely affect the rights and freedoms of those third parties.

Generally speaking, providing third party data to the individual making the portability request should not be a problem, assuming that the requestor provided this data to you within their information in the first place. However, you should always consider whether there will be an adverse effect on the rights and freedoms of third parties, in particular when you are transmitting data directly to another controller.

If the requested data has been provided to you by multiple data subjects (eg a joint bank account) you need to be satisfied that all parties agree to the portability request. This means that you may have to seek agreement from all the parties involved.

What is an individual entitled to?

The right to data portability entitles an individual to:

- receive a copy of their personal data; and/or
- have their personal data transmitted from one controller to another controller.

Individuals have the right to receive their personal data and store it for further personal use. This allows the individual to manage and reuse their personal data. For example, an individual wants to retrieve their contact list from a webmail application to build a wedding list or to store their data in a personal data store.

You can achieve this by either:

- directly transmitting the requested data to the individual; or
- providing access to an automated tool that allows the individual to extract the requested data themselves.

This does not create an obligation for you to allow individuals more general and routine access to your systems – only for the extraction of their data following a portability request.

You may have a preferred method of providing the information requested depending on the amount and complexity of the data requested. In either case, you need to ensure that the method is secure.

What are the limits when transmitting personal data to another controller?

Individuals have the right to ask you to transmit their personal data directly to another controller without hindrance. If it is technically feasible, you should do this.

You should consider the **technical feasibility** of a transmission on a request by request basis. The right to data portability does not create an obligation for you to adopt or maintain processing systems which are technically compatible with those of other organisations (GDPR Recital 68). However, you should take a reasonable approach, and this should not generally create a barrier to transmission.

Without hindrance means that you should not put in place any legal, technical or financial obstacles which slow down or prevent the transmission of the personal data to the individual, or to another organisation.

However, there may be legitimate reasons why you cannot undertake the transmission. For example, if the transmission would adversely affect the rights and freedoms of others. It is however your responsibility to justify why these reasons are legitimate and why they are not a ‘hindrance’ to the transmission.

Do we have responsibility for the personal data we transmit to others?

If you provide information directly to an individual or to another organisation in response to a data portability request, you are not responsible for any subsequent processing carried out by the individual or the other organisation. However, you are responsible for the transmission of the data and need to take appropriate measures to ensure that it is transmitted securely and to the right destination.

If you provide data to an individual, it is possible that they will store the information in a system with less security than your own. Therefore, you should make individuals aware of this so that they can take steps to protect the information they have received.

You also need to ensure that you comply with the other provisions in the GDPR. For example, whilst there is no specific obligation under the right to data portability to check and verify the quality of the data you transmit, you should already have taken reasonable steps to ensure the accuracy of this data in order to comply with the requirements of the accuracy principle of the GDPR.

How should we provide the data?

You should provide the personal data in a format that is:

- structured;
- commonly used; and
- machine-readable.

Although these terms are not defined in the GDPR these three characteristics can help you decide whether the format you intend to use is appropriate.

You can also find relevant information in the 'Open Data Handbook', published by Open Knowledge International. The handbook is a guide to 'open data', information that is free to access and can be re-used for any purpose – particularly information held by the public sector. The handbook contains a number of definitions that are relevant to the right to data portability, and this guidance includes some of these below.

What does 'structured' mean?

Structured data allows for easier transfer and increased usability.

The Open Data Handbook defines 'structured data' as:

> 'data where the structural relation between elements is explicit in the way the data is stored on a computer disk.'

This means that software must be able to extract specific elements of the data. An example of a structured format is a spreadsheet, where the data is organised into rows and columns, ie it is 'structured'. In practice, some of the personal data you process will already be in structured form.

In many cases, if a format is structured it is also machine-readable.

What does ‘commonly used’ mean?

This simply means that the format you choose must be widely-used and well-established.

However, just because a format is ‘commonly used’ does not mean it is appropriate for data portability. You have to consider whether it is ‘structured’, and ‘machine-readable’ as well. Although you may be using common software applications, which save data in commonly-used formats, these may not be sufficient to meet the requirements of data portability.

What does ‘machine-readable’ mean?

The Open Data Handbook states that ‘machine readable’ data is:

> ‘Data in a data format that can be automatically read and processed by a computer.’

Furthermore, Regulation 2 of the Re-use of Public Sector Information Regulations 2015 defines ‘machine-readable format’ as:

> ‘A file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure.’

Machine-readable data can be made directly available to applications that request that data over the web. This is undertaken by means of an application programming interface (“API”).

If you are able to implement such a system then you can facilitate data exchanges with individuals and respond to data portability requests in an easy manner.

Should we use an ‘interoperable’ format?

Although you are not required to use an interoperable format, this is encouraged by the GDPR, which seeks to promote the concept of interoperability. Recital 68 says:

> ‘Data controllers should be encouraged to develop interoperable formats that enable data portability.’

Interoperability allows different systems to share information and resources. An ‘interoperable format’ is a type of format that allows data to be exchanged between different systems and be understandable to both.

At the same time, you are not expected to maintain systems that are technically compatible with those of other organisations. Data portability is intended to produce interoperable systems, not compatible ones.

What formats can we use?

You may already be using an appropriate format within your networks and systems, and/or you may be required to use a particular format due to the particular industry or sector you are part of. Provided it meets the requirements of being structured, commonly-used and machine readable then it could be appropriate for a data portability request.

The GDPR does not require you to use open formats internally. Your processing systems may indeed use proprietary formats which individuals may not be able to access if you provide data to them in these formats. In these cases you need to perform some additional processing on the personal data in order to put it into the type of format required by the GDPR.

Where no specific format is in common use within your industry or sector, you should provide personal data using open formats such as CSV, XML and JSON. You may also find that these formats are the easiest for you to use when answering data portability requests.

For further information on CSV, XML and JSON, please see below.

What is CSV?

CSV stands for 'Comma Separated Values'. It is defined by the Open Data Handbook as:

> 'a standard format for spreadsheet data. Data is represented in a plain text file, with each data row on a new line and commas separating the values on each row. As a very simple open format it is easy to consume and is widely used for publishing open data.'

CSV is used to exchange data and is widely supported by software applications. Although CSV is not standardised it is nevertheless structured, commonly used and machine-readable and is therefore an appropriate format for you to use when responding to a data portability request.

What is XML?

XML stands for 'Extensible Markup Language'. It is defined by the Open Data Handbook as:

> 'a simple and powerful standard for representing structured data.'

It is a file format that is intended to be both human readable and machine-readable. Unlike CSV, XML is defined by a set of open standards maintained by the World Wide Web Consortium ("W3C"). It is widely used for documents, but can also be used to represent data structures such as those used in web

services.

This means XML can be processed by APIs, facilitating data exchange. For example, you may develop or implement an API to exchange personal data in XML format with another organisation. In the context of data portability, this can allow you to transmit personal data to an individual's personal data store, or to another organisation if the individual has asked you to do so.

What is JSON?

JSON stands for 'JavaScript Objection Notation'. The Open Data Handbook defines JSON as:

> 'a simple but powerful format for data. It can describe complex data structures, is highly machine-readable as well as reasonably human-readable, and is independent of platform and programming language, and is therefore a popular format for data interchange between programs and systems.'

It is a file format based on the JavaScript language that many web sites use and is used as a data interchange format. As with XML, it can be read by humans or machines. It is also a standardised open format maintained by the W3C

Are these the only formats we can use?

CSV, XML and JSON are three examples of structured, commonly used and machine-readable formats that are appropriate for data portability. However, this does not mean you are obliged to use them. Other formats exist that also meet the requirements of data portability.

Example

The RDF or 'Resource Description Framework' format is also a structured, commonly-used, machine-readable format. It is an open standard published by the W3C and is intended to provide interoperability between applications exchanging information.

You should however consider the nature of the portability request. If the individual cannot make use of the format, even if it is structured, commonly-used and machine-readable then the data will be of no use to them.

Further reading

The Open Data Handbook is published by Open Knowledge International and is a guide to 'open data'. The Handbook is updated regularly and you can read it here:

http://opendatahandbook.org

W3C candidate recommendation for XML is available here:

http://www.w3.org/TR/2008/REC-xml-20081126/

W3C's specification of the JSON data interchange format is available here:

https://tools.ietf.org/html/rfc7159

W3C's list of specifications for RDF is available here:

http://www.w3.org/standards/techs/rdf#w3c_all

What responsibilities do we have when we receive personal data because of a data portability request?

When you receive personal data that has been transmitted as part of a data portability request, you need to process this data in line with data protection requirements.

In deciding whether to accept and retain personal data, you should consider whether the data is relevant and not excessive in relation to the purposes for which you will process it. You also need to consider whether the data contains any third party information.

As a new controller, you need to ensure that you have an appropriate lawful basis for processing any third party data and that this processing does not adversely affect the rights and freedoms of those third parties. If you have received personal data which you have no reason to keep, you should delete it as soon as possible. When you accept and retain data, it becomes your responsibility to ensure that you comply with the requirements of the GDPR.

In particular, if you receive third party data you should not use this for your own purposes. You should keep the third party data under the sole control of the individual who has made the portability request, and only used for their own purposes.

Example

An individual enters into a contract with a controller for the provision of a service. The controller relies on Article 6(1)(b) to process the individual's personal data. The controller receives information from a data portability request that includes information about third parties. The controller has a legitimate interest to process the third party data under Article 6(1)(f) so that it can provide this service to the individual. However, it should not then use this data to send direct marketing to the third parties.

When can we refuse to comply with a request for data portability?

You can refuse to comply with a request for data portability if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If you consider that a request is manifestly unfounded or excessive you can:

- request a "reasonable fee" to deal with the request; or

- refuse to deal with the request.

In either case you will need to justify your decision.

You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

In more detail – Data Protection Bill

There are other proposed exemptions from the right to data portability that are contained in the draft DP Bill. As proposed, these exemptions will apply in certain circumstances, broadly associated with why you are processing the data. Once the DP Bill is finalised, we will update our guidance accordingly, and provide further detail on the application of these exemptions.

What should we do if we refuse to comply with a request for data portability?

You must inform the individual without undue delay and within one month of receipt of the request.

You should inform the individual about:

- the reasons you are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

How do we recognise a request?

The GDPR does not specify how individuals should make data portability requests. Therefore, requests could be made verbally or in writing. They can also be made to any part of your organisation and do not have to be to a specific person or contact point.

A request does not have to include the phrase 'request for data portability' or a reference to ‘Article 20 of the GDPR’, as long as one of the conditions listed above apply.

This presents a challenge as any of your employees could receive a valid request. However, you have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore you may need to consider which of your staff who regularly interact with individuals may need specific training to identify a request.

Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request. We also recommend that you keep a log of verbal requests.

In practice, you may already have processes in place to enable your staff to recognise subject access requests, such as training or established procedures. You could consider adapting them to ensure your

staff also recognise data portability requests.

Can we charge a fee?

No, in most cases you cannot charge a fee to comply with a request for data portability.

However, as noted above, if the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.

How long do we have to comply?

You must act upon the request without undue delay and at the latest within one month of receipt.

You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

Example

An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 4 October to comply with the request.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.

If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

Example

An organisation receives a request on 30 March. The time limit starts from the next day (31 March). As there is no equivalent date in April, the organisation has until 30 April to comply with the request.

If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.

For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Can we extend the time for a response?

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- you are requesting proof of identity before considering the request.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

You need to let the individual know as soon as possible that you need more information from them to confirm their identity before responding to their request. The period for responding to the request begins when you receive the additional information.

Further Reading

Relevant provisions in the GDPR - See Articles 13, 20 and Recital 68
External link

In more detail – Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The Article 29 Working Party has published guidelines and FAQs on data portability for organisations.

Right to object

At a glance

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

In brief

How do I comply with the right to object if I process personal data for the performance of a legal task or my organisation's legitimate interests?

Individuals must have an objection on "grounds relating to his or her particular situation".

You must stop processing the personal data unless:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

How do I comply with the right to object if I process personal data for direct marketing purposes?

You must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.

You must deal with an objection to processing for direct marketing at any time and free of charge.

You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

How do I comply with the right to object if I process personal data for research purposes?

Individuals must have "grounds relating to his or her particular situation" in order to exercise their right

to object to processing for research purposes.

If you are conducting research where the processing of personal data is necessary for the performance of a public interest task, you are not required to comply with an objection to the processing.

How do I comply with the right to object if my processing activities fall into any of the above categories and are carried out online?

You must offer a way for individuals to object online.

Further Reading

Relevant provisions in the GDPR - see Articles 12 and 21 and Recitals 69 and 70
External link

Rights related to automated decision making including profiling

At a glance

- The GDPR has provisions on:
  - automated individual decision-making (making a decision solely by automated means without any human involvement); and
  - profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.
- The GDPR applies to all automated individual decision-making and profiling.
- Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.
- You can only carry out this type of decision-making where the decision is:
  - necessary for the entry into or performance of a contract; or
  - authorised by Union or Member state law applicable to the controller; or
  - based on the individual's explicit consent.
- You must identify whether any of your processing falls under Article 22 and, if so, make sure that you:
  - give individuals information about the processing;
  - introduce simple ways for them to request human intervention or challenge a decision;
  - carry out regular checks to make sure that your systems are working as intended.

Checklists

All automated individual decision-making and profiling

To comply with the GDPR...

☐ We have a lawful basis to carry out profiling and/or automated decision-making and document this in our data protection policy.

☐ We send individuals a link to our privacy statement when we have obtained their personal data indirectly.

☐ We explain how people can access details of the information we used to create their profile.

☐ We tell people who provide us with their personal data how they can object to profiling, including profiling for marketing purposes.

☐ We have procedures for customers to access the personal data input into the profiles so they

can review and edit for any accuracy issues.

☐ We have additional checks in place for our profiling/automated decision-making systems to protect any vulnerable groups (including children).

☐ We only collect the minimum amount of data needed and have a clear retention policy for the profiles we create.

As a model of best practice...

☐ We carry out a DPIA to consider and address the risks before we start any new automated decision-making or profiling.

☐ We tell our customers about the profiling and automated decision-making we carry out, what information we use to create the profiles and where we get this information from.

☐ We use anonymised data in our profiling activities.

Solely automated individual decision-making, including profiling with legal or similarly significant effects (Article 22)

To comply with the GDPR...

☐ We carry out a DPIA to identify the risks to individuals, show how we are going to deal with them and what measures we have in place to meet GDPR requirements.

☐ We carry out processing under Article 22(1) for contractual purposes and we can demonstrate why it's necessary.

OR

☐ We carry out processing under Article 22(1) because we have the individual's explicit consent recorded. We can show when and how we obtained consent. We tell individuals how they can withdraw consent and have a simple way for them to do this.

OR

☐ We carry out processing under Article 22(1) because we are authorised or required to do so. This is the most appropriate way to achieve our aims.

☐ We don't use special category data in our automated decision-making systems unless we have a lawful basis to do so, and we can demonstrate what that basis is. We delete any special category data accidentally created.

☐ We explain that we use automated decision-making processes, including profiling. We explain what information we use, why we use it and what the effects might be.

☐ We have a simple way for people to ask us to reconsider an automated decision.

☐ We have identified staff in our organisation who are authorised to carry out reviews and change decisions.

☐ We regularly check our systems for accuracy and bias and feed any changes back into the design process.

As a model of best practice...

☐ We use visuals to explain what information we collect/use and why this is relevant to the process.

☐ We have signed up to [standard] a set of ethical principles to build trust with our customers. This is available on our website and on paper.

In brief

- What's new under the GDPR?
- What is automated individual decision-making and profiling?
- What does the GDPR say about automated individual decision-making and profiling?
- When can we carry out this type of processing?
- What else do we need to consider?
- What if Article 22 doesn't apply to our processing?

What's new under the GDPR?

- Profiling is now specifically defined in the GDPR.
- Solely automated individual decision-making, including profiling with legal or similarly significant effects is restricted.
- There are three grounds for this type of processing that lift the restriction.
- Where one of these grounds applies, you must introduce additional safeguards to protect data subjects. These work in a similar way to existing rights under the 1998 Data Protection Act.
- The GDPR requires you to give individuals specific information about automated individual decision-making, including profiling.
- There are additional restrictions on using special category and children's personal data.

What is automated individual decision-making and profiling?

Automated individual decision-making is a decision made by automated means without any human involvement.

Examples of this include:

- an online decision to award a loan; and
- a recruitment aptitude test which uses pre-programmed algorithms and criteria.

Automated individual decision-making does not have to involve profiling, although it often will do.

The GDPR says that profiling is:

> “Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.”
>
> [Article 4(4)]

Organisations obtain personal information about individuals from a variety of different sources. Internet searches, buying habits, lifestyle and behaviour data gathered from mobile phones, social networks, video surveillance systems and the Internet of Things are examples of the types of data organisations might collect.

Information is analysed to classify people into different groups or sectors, using algorithms and machine-learning. This analysis identifies links between different behaviours and characteristics to create profiles for individuals. There is more information about algorithms and machine-learning in our paper on big data, artificial intelligence, machine learning and data protection.

Based on the traits of others who appear similar, organisations use profiling to:

- find something out about individuals’ preferences;
- predict their behaviour; and/or
- make decisions about them.

This can be very useful for organisations and individuals in many sectors, including healthcare, education, financial services and marketing.

Automated individual decision-making and profiling can lead to quicker and more consistent decisions. But if they are used irresponsibly there are significant risks for individuals. The GDPR provisions are designed to address these risks.

What does the GDPR say about automated individual decision-making and profiling?

The GDPR restricts you from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals.

> “The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”
>
> [Article 22(1)]

For something to be solely automated there must be no human involvement in the decision-making process.

The restriction only covers solely automated individual decision-making that produces legal or similarly significant effects. These types of effect are not defined in the GDPR, but the decision must have a serious negative impact on an individual to be caught by this provision.

A legal effect is something that adversely affects someone's legal rights. Similarly significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention.

When can we carry out this type of processing?

Solely automated individual decision-making - including profiling - with legal or similarly significant effects is restricted, although this restriction can be lifted in certain circumstances.

You can **only** carry out solely automated decision-making with legal or similarly significant effects if the decision is:

- necessary for entering into or performance of a contract between an organisation and the individual;
- authorised by law (for example, for the purposes of fraud or tax evasion); or
- based on the individual's explicit consent.

If you're using special category personal data you can **only** carry out processing described in Article 22(1) if:

- you have the individual's explicit consent; **or**
- the processing is necessary for reasons of substantial public interest.

What else do we need to consider?

Because this type of processing is considered to be high-risk the GDPR requires you to carry out a Data Protection Impact Assessment (DPIA) to show that you have identified and assessed what those risks are and how you will address them.

As well as restricting the circumstances in which you can carry out solely automated individual decision-making (as described in Article 22(1)) the GDPR also:

- requires you to give individuals specific information about the processing;
- obliges you to take steps to prevent errors, bias and discrimination; and
- gives individuals rights to challenge and request a review of the decision.

These provisions are designed to increase individuals' understanding of how you might be using their personal data.

You must:

- provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual;
- use appropriate mathematical or statistical procedures;
- ensure that individuals can:
  - obtain human intervention;

  - express their point of view; and
  - obtain an explanation of the decision and challenge it;
- put appropriate technical and organisational measures in place, so that you can correct inaccuracies and minimise the risk of errors;
- secure personal data in a way that is proportionate to the risk to the interests and rights of the individual, and that prevents discriminatory effects.

What if Article 22 doesn't apply to our processing?

Article 22 applies to solely automated individual decision-making, including profiling, with legal or similarly significant effects.

If your processing does not match this definition then you can continue to carry out profiling and automated decision-making.

But you must still comply with the GDPR principles.

You must identify and record your lawful basis for the processing.

You need to have processes in place so people can exercise their rights.

Individuals have a right to object to profiling in certain circumstances. You must bring details of this right specifically to their attention.

Further Reading

Relevant provisions in the GDPR - Article 4(4), 9, 12, 13, 14, 15, 21, 22, 35(1)and (3)
External link

In more detail – ICO guidance

We are planning to publish more detailed practical guidance on this topic shortly.

Privacy notices transparency and control

Big data, artificial intelligence, machine learning and data protection

In more detail – Article 29

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

Following the consultation period, the Article 29 Working Party has adopted final guidelines on Automated individual decision-making and Profiling.

Other relevant guidelines published by WP29 include:

WP29 guidelines on Data Protection Impact Assessment

Accountability and governance

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.

In brief

- What's new under the GDPR?
- What is accountability?
- Why is accountability important?
- What do we need to do?
- Should we implement data protection policies?
- Should we adopt a 'data protection by design and default' approach?
- Do we need to use contracts?
- What documentation should we maintain?
- What security measures should we put in place?
- How do we record and report personal data breaches?
- Should we carry out data protection impact assessments (DPIAs)?
- Should we assign a data protection officer (DPO)?
- Should we adhere to codes of conduct and certification schemes?
- What else should we consider?

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. Although these obligations were implicit in the Data Protection Act 1998 (1998 Act), the GDPR makes them explicit.

You now need to be proactive about data protection, and evidence the steps you take to meet your obligations and protect people's rights. Good practice tools that the ICO has championed for a long time, such as privacy impact assessments and privacy by design, are now formally recognised and legally required in some circumstances.

Organisations that already adopt a best practice approach to compliance with the 1998 Act should not find it too difficult to adapt to the new requirements. But you should review the measures you take to comply with the 1998 Act, update them for the GDPR if necessary, and stand ready to demonstrate your compliance under the GDPR.

Further Reading

Relevant provisions in the GDPR - See Articles 5 and 24, and Recitals 39 and 74
External link

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.

Article 5(2) of the GDPR says:

> "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 [the other data protection principles]"

Further Reading

Relevant provisions in the GDPR - See Article 5 and Recital 39
External link

Further reading – ICO guidance

Principles

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.

Further Reading

Relevant provisions in the GDPR - See Article 83
External link

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. Amongst other things, your framework should include:

- robust program controls informed by the requirements of the GDPR;
- appropriate reporting structures; and
- assessment and evaluation procedures.

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.

Article 24(1) of the GDPR says that:

- you must implement technical and organisational measures to ensure, and demonstrate, compliance with the GDPR;
- the measures should be risk-based and proportionate; and
- you need to review and update the measures as necessary.

While the GDPR does not specify an exhaustive list of things you need to do to be accountable, it does set out several different measures you can take that will help you get there. These are summarised under the headings below, with links to the relevant parts of the guide. 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 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. This could include awareness raising, training, monitoring and audits – all tasks that your data protection officer can undertake (see below for more on data protection officers).

Further Reading

Relevant provisions in the GDPR - See Articles 24(2) and Recital 78
External link

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.

Integrating data protection considerations into your operations helps you to comply with your obligations, while documenting the decisions you take (often in data protection impact assessments – see below) demonstrates this.

Further Reading

Relevant provisions in the GDPR - See Article 25 and Recital 78
External link

Further reading – ICO guidance

Data protection by design and default

Anonymisation code of practice

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.

Using clear and comprehensive contracts with your processors helps to ensure that everyone understands their data protection obligations and is a good way to demonstrate this formally.

Further Reading

Relevant provisions in the GDPR - See Article 28 and Recital 81
External link

Further reading – ICO guidance

Contracts

What documentation should we maintain?

Under Article 30 of the GDPR, 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.

Further Reading

Relevant provisions in the GDPR - See Articles 7(1), 30 and 33(5), and Recitals 42 and 82
External link

Further reading – ICO guidance

Documentation

Consent

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.

Further Reading

Relevant provisions in the GDPR - See Articles 5(f) and 32, and Recitals 39 and 83
External link

Further reading – ICO guidance

Security

How do we record and report personal data breaches?

You must report certain types of personal data breach to the relevant supervisory authority (for the UK, this is the ICO), 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 helps you do this.

Further Reading

Relevant provisions in the GDPR - See Articles 33-34 and Recitals 85-88
External link

Further reading – ICO guidance

Personal data breaches

Further reading – Article 29

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 guidelines on Personal data breach notification

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.

Further Reading

Relevant provisions in the GDPR - See Articles 35-36, and Recitals 84 and 89-95
External link

Further reading – ICO guidance

Data protection impact assessments

Further reading – Article 29

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 guidelines on Data Protection Impact Assessments

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.

Further Reading

Relevant provisions in the GDPR - See Articles 37-39, and Recital 97
External link

Further reading – ICO guidance

Data protection officers

Further reading – Article 29

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 guidelines on Data Protection Officers

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 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.

Further Reading

Relevant provisions in the GDPR - See Articles 40-43, and Recitals 98 and 100
External link

Further reading – ICO guidance

Codes of conduct and certification

What else should we consider?

The above measures can help to support an accountable approach to data protection, but it is not limited to these. You need to be able to prove what steps you have taken to comply. In practice this means keeping records of what you do and justifying your decisions.

Example

A company wants to use the personal data it holds for a new purpose. It carries out an assessment

in line with Article 6(4) of the GDPR, and determines that the new purpose is compatible with the original purpose for which it collected the personal data. Although this provision of the GDPR does not specify that the company must document its compatibility assessment, it knows that to be accountable, it needs to be able to prove that their handling of personal data is compliant with the GDPR. The company therefore keeps a record of the compatibility assessment, including its rationale for the decision and the appropriate safeguards it put in place.

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 who 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.

Further Reading

Relevant provisions in the GDPR - See Articles 12-14, 22 and 24(1), and Recitals 39, 58-61 and 71

External link

Further reading – ICO guidance

Right to be informed

Rights related to automated decision making including profiling

Data protection self assessment

Contracts

At a glance

- Whenever a controller uses a processor it needs to have a written contract in place.
- The contract is important so that both parties understand their responsibilities and liabilities.
- The GDPR sets out what needs to be included in the contract.
- In the future, standard contract clauses may be provided by the European Commission or the ICO, and may form part of certification schemes. However at the moment no standard clauses have been drafted.
- Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. In the future, using a processor which adheres to an approved code of conduct or certification scheme may help controllers to satisfy this requirement – though again, no such schemes are currently available.
- Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

Checklists

Controller and processor contracts checklist

Our contracts include the following compulsory details:

☐ the subject matter and duration of the processing;

☐ the nature and purpose of the processing;

☐ the type of personal data and categories of data subject; and

☐ the obligations and rights of the controller.

Our contracts include the following compulsory terms:

☐ the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);

☐ the processor must ensure that people processing the data are subject to a duty of confidence;

☐ the processor must take appropriate measures to ensure the security of processing;

☐ the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;

☐ the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;

☐ the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;

☐ the processor must delete or return all personal data to the controller as requested at the end of the contract; and

☐ the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

As a matter of good practice, our contracts:

☐ state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR; and

☐ reflect any indemnity that has been agreed.

Processors' responsibilities and liabilities checklist

In addition to the Article 28.3 contractual obligations set out in the controller and processor contracts checklist, a processor has the following direct responsibilities under the GDPR. The processor must:

☐ only act on the written instructions of the controller (Article 29);

☐ not use a sub-processor without the prior written authorisation of the controller (Article 28.2);

☐ co-operate with supervisory authorities (such as the ICO) in accordance with Article 31;

☐ ensure the security of its processing in accordance with Article 32;

☐ keep records of its processing activities in accordance with Article 30.2;

☐ notify any personal data breaches to the controller in accordance with Article 33;

☐ employ a data protection officer if required in accordance with Article 37; and

☐ appoint (in writing) a representative within the European Union if required in accordance with Article 27.

A processor should also be aware that:

☐ it may be subject to investigative and corrective powers of supervisory authorities (such as the ICO) under Article 58 of the GDPR;

☐ if it fails to meet its obligations, it may be subject to an administrative fine under Article 83 of the GDPR;

☐ if it fails to meet its GDPR obligations it may be subject to a penalty under Article 84 of the GDPR; and

☐ if it fails to meet its GDPR obligations it may have to pay compensation under Article 82 of the GDPR.

In brief

What's new?

- The GDPR makes written contracts between controllers and processors a general requirement, rather than just a way of demonstrating compliance with the seventh data protection principle (appropriate security measures) under the DPA.
- These contracts must now include certain specific terms, as a minimum.
- These terms are designed to ensure that processing carried out by a processor meets all the requirements of the GDPR (not just those related to keeping personal data secure).
- The GDPR allows for standard contractual clauses from the EU Commission or a supervisory authority (such as the ICO) to be used in contracts between controllers and processors - though none have been drafted so far.

- The GDPR envisages that adherence by a processor to an approved code of conduct or certification scheme may be used to help controllers demonstrate that they have chosen a suitable processor. Standard contractual clauses may form part of such a code or scheme, though again, no schemes are currently available.
- The GDPR gives processors responsibilities and liabilities in their own right, and processors as well as controllers may now be liable to pay damages or be subject to fines or other penalties.

When is a contract needed?

Whenever a controller uses a processor (a third party who processes personal data on behalf of the controller) it needs to have a written contract in place. Similarly, if a processor employs another processor it needs to have a written contract in place.

Why are contracts between controllers and processors important?

Contracts between controllers and processors ensure that they both understand their obligations, responsibilities and liabilities. They help them to comply with the GDPR, and help controllers to demonstrate their compliance with the GDPR. The use of contracts by controllers and processors may also increase data subjects' confidence in the handling of their personal data.

What needs to be included in the contract?

Contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller.

Contracts must also include as a minimum the following terms, requiring the processor to:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Can standard contracts clauses be used?

The GDPR allows standard contractual clauses from the EU Commission or a Supervisory Authority (such as the ICO) to be used in contracts between controllers and processors. However, no standard clauses are currently available.

The GDPR also allows these standard contractual clauses to form part of a code of conduct or certification mechanism to demonstrate compliant processing. However, no schemes are currently available.

What responsibilities and liabilities do processors have in their own right?

A processor must only act on the documented instructions of a controller. If a processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a controller and will have the same liability as a controller.

In addition to its contractual obligations to the controller, under the GDPR a processor also has the following direct responsibilities:

- not to use a sub-processor without the prior written authorisation of the data controller;
- to co-operate with supervisory authorities (such as the ICO);
- to ensure the security of its processing;
- to keep records of processing activities;
- to notify any personal data breaches to the data controller;
- to employ a data protection officer; and
- to appoint (in writing) a representative within the European Union if needed.

If a processor fails to meet any of these obligations, or acts outside or against the instructions of the controller, then it may be liable to pay damages in legal proceedings, or be subject to fines or other penalties or corrective measures.

If a processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor's obligations.

Further Reading

Relevant provisions in the GDPR - see Articles 28-36 and Recitals 81-83
External link

In more detail – ICO guidance

The deadline for responses to our draft GDPR guidance on contracts and liabilities for controllers and processors has now passed. We are analysing the feedback and this will feed into the final version.

Documentation

At a glance

- The GDPR contains explicit provisions about documenting your processing activities.
- You must maintain records on several things such as processing purposes, data sharing and retention.
- You may be required to make the records available to the ICO on request.
- Documentation can help you comply with other aspects of the GDPR and improve your data governance.
- Controllers and processors both have documentation obligations.
- For small and medium-sized organisations, documentation requirements are limited to certain types of processing activities.
- Information audits or data-mapping exercises can feed into the documentation of your processing activities.
- Records must be kept in writing.
- Most organisations will benefit from maintaining their records electronically.
- Records must be kept up to date and reflect your current processing activities.
- We have produced some basic templates to help you document your processing activities.

Checklists

Documentation of processing activities – requirements

☐ If we are a controller for the personal data we process, we document all the applicable information under Article 30(1) of the GDPR.

☐ If we are a processor for the personal data we process, we document all the applicable information under Article 30(2) of the GDPR.

If we process special category or criminal conviction and offence data, we document:

- ☐ the condition for processing we rely on in the Data Protection Bill;
- ☐ the lawful basis for our processing; and
- ☐ whether we retain and erase the personal data in accordance with our policy document.

☐ We document our processing activities in writing.

☐ We document our processing activities in a granular way with meaningful links between the different pieces of information.

☐ We conduct regular reviews of the personal data we process and update our documentation accordingly.

Documentation of processing activities – best practice

When preparing to document our processing activities we:

☐ do information audits to find out what personal data our organisation holds;

☐ distribute questionnaires and talk to staff across the organisation to get a more complete picture of our processing activities; and

☐ review our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

As part of our record of processing activities we document, or link to documentation, on:

☐ information required for privacy notices;

☐ records of consent;

☐ controller-processor contracts;

☐ the location of personal data;

☐ Data Protection Impact Assessment reports; and

☐ records of personal data breaches.

☐ We document our processing activities in electronic form so we can add, remove and amend information easily.

In brief

- What's new under the GDPR?
- What is documentation?
- Who needs to document their processing activities?
- What do we need to document under Article 30 of the GDPR?
- Should we document anything else?
- How do we document our processing activities?

What's new under the GDPR?

- The documentation of processing activities is a new requirement under the GDPR.
- There are some similarities between documentation under the GDPR and the information you provided to the ICO as part of registration under the Data Protection Act 1998.
- You need to make sure that you have in place a record of your processing activities by 25 May 2018.

What is documentation?

- Most organisations are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention; we call this **documentation**.
- Documenting your processing activities 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.

Who needs to document their processing activities?

- Controllers and processors each have their own documentation obligations.
- If you have 250 or more employees, you must document all your processing activities.
- There is a limited exemption for small and medium-sized organisations. If you have fewer than 250 employees, you only need to document processing activities that:
  - are not occasional; or
  - could result in a risk to the rights and freedoms of individuals; or
  - involve the processing of special categories of data or criminal conviction and offence data.

What do we need to document under Article 30 of the GDPR?

You must document the following information:

- The name and contact details of your organisation (and where applicable, of other controllers, your representative and your data protection officer).
- The purposes of your processing.
- A description of the categories of individuals and categories of personal data.
- The categories of recipients of personal data.
- Details of your transfers to third countries including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- A description of your technical and organisational security measures.

Should we document anything else?

As part of your record of processing activities, it can be useful to document (or link to documentation of) other aspects of your compliance with the GDPR and the UK's Data Protection Bill. Such documentation may include:

- information required for privacy notices, such as:
  - the lawful basis for the processing
  - the legitimate interests for the processing
  - individuals' rights
  - the existence of automated decision-making, including profiling
  - the source of the personal data;
- records of consent;

- controller-processor contracts;
- the location of personal data;
- Data Protection Impact Assessment reports;
- records of personal data breaches;
- information required for processing special category data or criminal conviction and offence data under the Data Protection Bill, covering:
  - the condition for processing in the Data Protection Bill
  - the lawful basis for the processing in the GDPR
  - your retention and erasure policy document.

How do we document our processing activities?

- Doing an information audit or data-mapping exercise can help you find out what personal data your organisation holds and where it is.
- You can find out why personal data is used, who it is shared with and how long it is kept by distributing questionnaires to relevant areas of your organisation, meeting directly with key business functions, and reviewing policies, procedures, contracts and agreements.
- When documenting your findings, the records you keep must be in writing. The information must be documented in a granular and meaningful way.

We have developed basic templates to help you document your processing activities.

Further Reading

Documentation template for controllers
For organisations
File (34.42K)

Documentation template for processors
For organisations
File (19.48K)

Further Reading

Relevant provisions in the GDPR – See Article 30 and Recital 82
External link

Relevant provisions in the Data Protection Bill – See Schedule 1
External link

In more detail – ICO guidance

We have produced more detailed guidance on documentation.

In more detail - Article 29

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 has published a position paper on Article 30(5) (the exemption for small and medium-sized organisations).

Data protection by design and default

At a glance

- Under the GDPR, you have a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities.
- Privacy by design has always been an implicit requirement of data protection that the ICO has consistently championed.
- The ICO has published guidance on privacy by design. We are working to update this guidance to reflect the provisions of the GDPR. In the meantime, the existing guidance is a good starting point for organisations.

Data protection impact assessments

At a glance

- A data protection impact assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.
- You must do a DPIA for certain listed types of processing, or any other processing that is **likely to result in a high risk** to individuals' interests. You can use our screening checklist to help you decide when to do a DPIA.
- It is also good practice to do a DPIA for any other major project which requires the processing of personal data.
- Your DPIA must:
  - describe the nature, scope, context and purposes of the processing;
  - assess necessity, proportionality and compliance measures;
  - identify and assess risks to individuals; and
  - identify any additional measures to mitigate those risks.
- To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.
- You should consult your DPO (if you have one) and, where appropriate, individuals and relevant experts. Processors may need to assist.
- If you identify a high risk and you cannot mitigate that risk, you must consult the ICO before starting the processing.
- The ICO will give written advice within eight weeks, or 14 weeks in complex cases. In appropriate cases we may issue a formal warning not to process the data, or ban the processing altogether.

Checklists

DPIA awareness checklist

☐ We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.

☐ Our existing policies, processes and procedures include references to DPIA requirements.

☐ We understand the types of processing that require a DPIA, and use the screening checklist to identify the need for a DPIA where necessary.

☐ We have created and documented a DPIA process.

☐ We provide training for relevant staff on how to carry out a DPIA.

DPIA screening checklist

☐ We always carry out a DPIA if we plan to:

- ☐ Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
- ☐ Process special category data or criminal offence data on a large scale.
- ☐ Systematically monitor a publicly accessible place on a large scale.
- ☐ Use new technologies.
- ☐ Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
- ☐ Carry out profiling on a large scale.
- ☐ Process biometric or genetic data.
- ☐ Combine, compare or match data from multiple sources.
- ☐ Process personal data without providing a privacy notice directly to the individual.
- ☐ Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
- ☐ Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- ☐ Process personal data which could result in a risk of physical harm in the event of a security breach.

☐ We consider carrying out a DPIA if we plan to carry out any other:

- ☐ Evaluation or scoring.
- ☐ Automated decision-making with significant effects.
- ☐ Systematic monitoring.
- ☐ Processing of sensitive data or data of a highly personal nature.
- ☐ Processing on a large scale.
- ☐ Processing of data concerning vulnerable data subjects.
- ☐ Innovative technological or organisational solutions.
- ☐ Processing involving preventing data subjects from exercising a right or using a service or contract.

☐ If we decide not to carry out a DPIA, we document our reasons.

☐ We consider carrying out a DPIA in any major project involving the use of personal data.

☐ We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

DPIA process checklist

☐ We describe the nature, scope, context and purposes of the processing.

☐ We ask our data processors to help us understand and document their processing activities and identify any associated risks.

☐ We consider how best to consult individuals (or their representatives) and other relevant stakeholders.

☐ We ask for the advice of our data protection officer.

☐ We check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure data protection compliance.

☐ We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.

☐ We identify measures we can put in place to eliminate or reduce high risks.

☐ We record the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.

☐ We implement the measures identified, and integrate them into our project plan.

☐ We consult the ICO before processing if we cannot mitigate high risks.

☐ We keep our DPIAs under review and revisit them if necessary.

In brief

- What's new under the GDPR?
- What is a DPIA?
- When do we need to do a DPIA?
- How do we carry out a DPIA?
- Do we need to consult the ICO?

What's new under the GDPR?

The GDPR introduces a new obligation to do a DPIA before carrying out processing likely to result in high risk to individuals' interests. If your DPIA identifies a high risk which you cannot mitigate, you must consult the ICO.

This is a key element of the new focus on accountability and data protection by design, and a more risk-based approach to compliance.

Some organisations will already carry out privacy impact assessments (PIAs) as a matter of good practice. If so, you will need to review your processes to make sure they comply with GDPR requirements. The big changes are that DPIAs are now mandatory in some cases, and there are specific requirements for content and process.

If you have not already got a PIA process, you will need to design a new DPIA process and embed this into your organisational policies and procedures.

In the run-up to 25 May 2018, you also need to review your existing processing operations and decide whether you need to do a DPIA for anything which is likely to be high risk. You will not need to do a DPIA if you have already considered the relevant risks and safeguards, unless there has been a significant change to the nature, scope, context or purposes of the processing.

What is a DPIA?

A DPIA is a process to systematically analyse your processing and help you identify and minimise data protection risks. It must:

- describe the processing and your purposes;
- assess necessity and proportionality;
- identify and assess risks to individuals; and
- identify any measures to mitigate those risks and protect the data.

It does not have to eradicate the risk, but should help to minimise risks and consider whether or not they are justified.

You must do a DPIA for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability more generally and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

It’s important to embed DPIAs into your organisational processes and ensure the outcome can influence your plans. A DPIA is not a one-off exercise and should be seen as an ongoing process, kept under regular review.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – whether physical, material or non-material - to individuals or to society at large.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It should look at risk based on the specific nature, scope, context and purposes of the processing.

When do we need to do a DPIA?

You must do a DPIA before you begin any type of processing which is “likely to result in a high risk”. This means that although the actual level of risk has not been assessed yet, you need to screen for factors which point to the potential for a widespread or serious impact on individuals.

In particular, the GDPR says you must do a DPIA if you plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

The ICO also requires you to do a DPIA if you plan to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

You should also think carefully about doing a DPIA for any other processing which is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

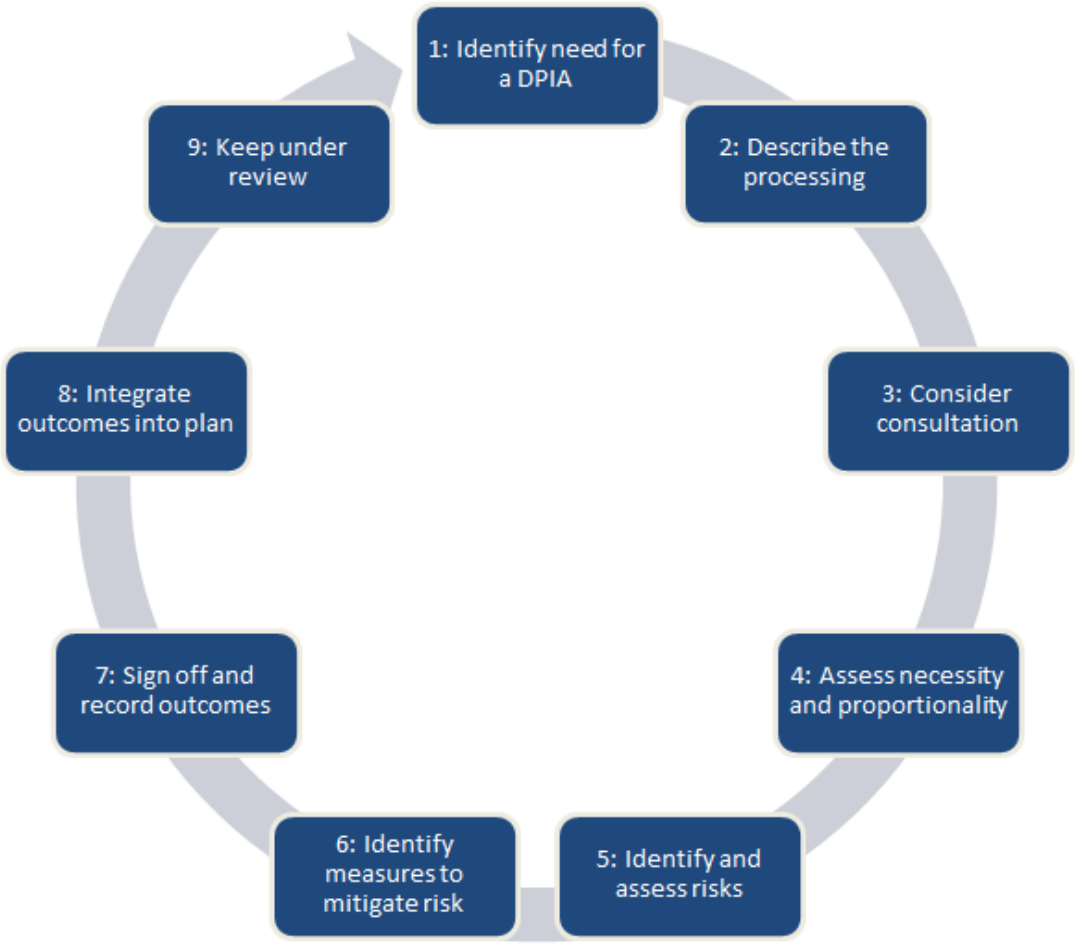
Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data.

Consultation – have your say

The ICO is required by Article 35(4) of the GDPR to publish a list of types of processing we consider likely to be high risk and so require a DPIA. Our list, which is summarised above, is currently open for consultation until 13 April 2018.

How do we carry out a DPIA?

A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process. It should include these steps:



You must seek the advice of your data protection officer (if you have one). You should also consult with individuals and other stakeholders throughout this process.

The process is designed to be flexible and scalable. You can use or adapt our sample DPIA template, or create your own. If you want to create your own, you may want to refer to the European guidelines which set out Criteria for an acceptable DPIA.

We recommend that you publish your DPIAs, with sensitive details removed if necessary.

Do we need to consult the ICO?

If you have carried out a DPIA that identifies a high risk, and you cannot take any measures to reduce this risk, you need to consult the ICO. You cannot go ahead with the processing until you have done so.

The focus is on the 'residual risk' after any mitigating measures have been taken. If your DPIA identified a high risk, but you have taken measures to reduce this risk so that it is no longer a high risk, you do not need to consult the ICO.

You need to complete our online form and submit a copy of your DPIA.

Once we have the information we need, we will generally respond within eight weeks (although we can extend this by a further six weeks in complex cases).

We will provide you with a written response advising you whether the risks are acceptable, or whether you need to take further action. In some cases we may advise you not to carry out the processing because we consider it would be in breach of the GDPR. In appropriate cases we may issue a formal

warning or take action to ban the processing altogether.

Further Reading

Key provisions in the GDPR - See Articles 35 and 36 and Recitals 74-77, 84, 89-92, 94 and 95
External link

Further reading – ICO guidance

We have published more detailed guidance on DPIAs. The content of this detailed guidance is subject to public consultation, which closes on 13 April 2018.

Further reading – Article 29 guidelines

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The working party has published Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248).

Other relevant guidelines include:

Guidelines on Data Protection Officers ('DPOs') (WP243)

Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251)

Data protection officers

At a glance

- The GDPR introduces a duty for you to appoint a data protection officer (DPO) if you are a public authority, or if you carry out certain types of processing activities.
- DPOs assist you to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.
- The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.
- A DPO can be an existing employee or externally appointed.
- In some cases several organisations can appoint a single DPO between them.
- DPOs can help you demonstrate compliance and are part of the enhanced focus on accountability.

Checklists

Appointing a DPO

☐ We are a public authority and have appointed a DPO (except if we are a court acting in our judicial capacity).

☐ We are not a public authority, but we know whether the nature of our processing activities requires the appointment of a DPO.

☐ We have appointed a DPO based on their professional qualities and expert knowledge of data protection law and practices.

☐ We aren’t required to appoint a DPO under the GDPR but we have decided to do so voluntarily. We understand that the same duties and responsibilities apply had we been required to appoint a DPO. We support our DPO to the same standards.

Position of the DPO

☐ Our DPO reports directly to our highest level of management and is given the required independence to perform their tasks.

☐ We involve our DPO, in a timely manner, in all issues relating to the protection of personal data.

☐ Our DPO is sufficiently well resourced to be able to perform their tasks.

☐ We do not penalise the DPO for performing their duties.

☐ We ensure that any other tasks or duties we assign our DPO do not result in a conflict of interests with their role as a DPO.

Tasks of the DPO

☐ Our DPO is tasked with monitoring compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits.

☐ We will take account of our DPO's advice and the information they provide on our data protection obligations.

☐ When carrying out a DPIA, we seek the advice of our DPO who also monitors the process.

☐ Our DPO acts as a contact point for the ICO. They co-operate with the ICO, including during prior consultations under Article 36, and will consult on any other matter.

☐ When performing their tasks, our DPO has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

Accessibility of the DPO

☐ Our DPO is easily accessible as a point of contact for our employees, individuals and the ICO.

☐ We have published the contact details of the DPO and communicated them to the ICO.

In brief

Do we need to appoint a Data Protection Officer?

Under the GDPR, you **must** appoint a DPO if:

- you are a public authority (except for courts acting in their judicial capacity);
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

This applies to both controllers and processors. You can appoint a DPO if you wish, even if you aren't required to. If you decide to voluntarily appoint a DPO you should be aware that the same requirements of the position and tasks apply had the appointment been mandatory.

Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and resources to discharge your obligations under the GDPR. However, a DPO can help you operate within the law by advising and helping to monitor compliance. In this way, a DPO can be seen to play a key role in your organisation's data protection governance structure and to help improve accountability.

If you decide that you don't need to appoint a DPO, either voluntarily or because you don't meet the above criteria, it's a good idea to record this decision to help demonstrate compliance with the accountability principle.

What is the definition of a public authority?

The Data Protection Bill will define what a 'public authority' is under GDPR. This is likely to be the same as those defined under the Freedom of Information Act 2000 (FOIA) or the Freedom of Information Act (Scotland) 2002.

This means that if you are already defined as a public authority or public body under FOIA or the Scottish FOIA, it's likely you will be a public authority under the GDPR. However, the Data Protection Bill is subject to amendment and so you should confirm your status when the Bill becomes an Act of Parliament.

What are 'core activities'?

The other two conditions that require you to appoint a DPO only apply when:

- your core activities consist of processing activities, which, by virtue of their nature, scope and / or their purposes, require the regular and systematic monitoring of individuals on a large scale; or
- your core activities consist of processing on a large scale of special category data, or data relating to criminal convictions and offences.

Your core activities are the primary business activities of your organisation. So, if you need to process personal data to achieve your key objectives, this is a core activity. This is different to processing personal data for other secondary purposes, which may be something you do all the time (eg payroll or HR information), but which is not part of carrying out your primary objectives.

Example

For most organisations, processing personal data for HR purposes will be a secondary function to their main business activities and so will not be part of their core activities.

However, a HR service provider necessarily processes personal data as part of its core activities to provide HR functions for its client organisations. At the same time, it will also process HR information for its own employees, which will be regarded as an ancillary function and not part of its core activities.

What does 'regular and systematic monitoring of data subjects on a large scale' mean?

There are two key elements to this condition requiring you to appoint a DPO. Although the GDPR does not define 'regular and systematic monitoring' or 'large scale', the Article 29 Working Party has provided some guidance on these terms in its guidelines on DPOs.

'Regular and systematic' monitoring of data subjects includes all forms of tracking and profiling, both online and offline. An example of this is for the purposes of behavioural advertising.

When determining if processing is on a large scale, the guidelines say you should take the following factors into consideration:

- the numbers of data subjects concerned;
- the volume of personal data being processed;
- the range of different data items being processed;
- the geographical extent of the activity; and
- the duration or permanence of the processing activity.

Example

A large retail website uses algorithms to monitor the searches and purchases of its users and, based on this information, it offers recommendations to them. As this takes place continuously and according to predefined criteria, it can be considered as regular and systematic monitoring of data subjects on a large scale.

What does processing special category data and personal data relating to criminal convictions and offences on a large scale mean?

Processing special category data or criminal conviction or offences data carries more risk than other personal data. So when you process this type of data on a large scale you are required to appoint a DPO, who can provide more oversight. Again, the factors relevant to large-scale processing can include:

- the numbers of data subjects;
- the volume of personal data being processed;
- the range of different data items being processed;
- the geographical extent of the activity; and
- the duration or permanence of the activity.

Example

A health insurance company processes a wide range of personal data about a large number of individuals, including medical conditions and other health information. This can be considered as processing special category data on a large scale.

What professional qualities should the DPO have?

- The GDPR says that you should appoint a DPO on the basis of their professional qualities, and in particular, experience and expert knowledge of data protection law.
- It doesn’t specify the precise credentials they are expected to have, but it does say that this should be proportionate to the type of processing you carry out, taking into consideration the level of

protection the personal data requires.

- So, where the processing of personal data is particularly complex or risky, the knowledge and abilities of the DPO should be correspondingly advanced enough to provide effective oversight.
- It would be an advantage for your DPO to also have a good knowledge of your industry or sector, as well as your data protection needs and processing activities.

What are the tasks of the DPO?

The DPO's tasks are defined in Article 39 as:

- to inform and advise you and your employees about your obligations to comply with the GDPR and other data protection laws;
- to monitor compliance with the GDPR and other data protection laws, and with your data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor, data protection impact assessments;
- to cooperate with the supervisory authority; and
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

It's important to remember that the DPO's tasks cover all personal data processing activities, not just those that require their appointment under Article 37(1).

- When carrying out their tasks the DPO is required to take into account the risk associated with the processing you are undertaking. They must have regard to the nature, scope, context and purposes of the processing.
- The DPO should prioritise and focus on the more risky activities, for example where special category data is being processed, or where the potential impact on individuals could be damaging. Therefore, DPOs should provide risk-based advice to your organisation.
- If you decide not to follow the advice given by your DPO, you should document your reasons to help demonstrate your accountability.

Can we assign other tasks to the DPO?

The GDPR says that you can assign further tasks and duties, so long as they don't result in a conflict of interests with the DPO's primary tasks.

Example

As an example of assigning other tasks, Article 30 requires that organisations must maintain records of processing operations. There is nothing preventing this task being allocated to the DPO.

Basically this means the DPO cannot hold a position within your organisation that leads him or her to determine the purposes and the means of the processing of personal data. At the same time, the DPO

shouldn’t be expected to manage competing objectives that could result in data protection taking a secondary role to business interests.

Examples

A company’s head of marketing plans an advertising campaign, including which of the company’s customers to target, what method of communication and the personal details to use. This person cannot also be the company’s DPO, as the decision-making is likely to lead to a conflict of interests between the campaign’s aims and the company’s data protection obligations.

On the other hand, a public authority could appoint its existing FOI officer / records manager as its DPO. There is no conflict of interests here as these roles are about ensuring information rights compliance, rather than making decisions about the purposes of processing.

Can the DPO be an existing employee?

Yes. As long as the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests, you can appoint an existing employee as your DPO, rather than you having to create a new post.

Can we contract out the role of the DPO?

You can contract out the role of DPO externally, based on a service contract with an individual or an organisation. It’s important to be aware that an externally-appointed DPO should have the same position, tasks and duties as an internally-appointed one.

Can we share a DPO with other organisations?

- You may appoint a single DPO to act for a group of companies or public authorities.
- If your DPO covers several organisations, they must still be able to perform their tasks effectively, taking into account the structure and size of those organisations. This means you should consider if one DPO can realistically cover a large or complex collection of organisations. You need to ensure they have the necessary resources to carry out their role and be supported with a team, if this is appropriate.
- Your DPO must be easily accessible, so their contact details should be readily available to your employees, to the ICO, and people whose personal data you process.

Can we have more than one DPO?

- The GDPR clearly provides that an organisation must appoint a single DPO to carry out the tasks required in Article 39, but this doesn’t prevent it appointing other data protection specialists as part of a team to help support the DPO.
- You need to determine the best way to set up your organisation’s DPO function and whether this necessitates a data protection team. However, there must be an individual designated as the DPO for

the purposes of the GDPR who meets the requirements set out in Articles 37-39.

- If you have a team, you should clearly set out the roles and responsibilities of its members and how it relates to the DPO.
- If you hire data protection specialists other than a DPO, it's important that they are not referred to as your DPO, which is a specific role with particular requirements under the GDPR.

What do we have to do to support the DPO?

You must ensure that:

- the DPO is involved, closely and in a timely manner, in all data protection matters;
- the DPO reports to the highest management level of your organisation, ie board level;
- the DPO operates independently and is not dismissed or penalised for performing their tasks;
- you provide adequate resources (sufficient time, financial, infrastructure, and, where appropriate, staff) to enable the DPO to meet their GDPR obligations, and to maintain their expert level of knowledge;
- you give the DPO appropriate access to personal data and processing activities;
- you give the DPO appropriate access to other services within your organisation so that they can receive essential support, input or information;
- you seek the advice of your DPO when carrying out a DPIA; and
- you record the details of your DPO as part of your records of processing activities.

This shows the importance of the DPO to your organisation and that you must provide sufficient support so they can carry out their role independently. Part of this is the requirement for your DPO to report to the highest level of management. This doesn't mean the DPO has to be line managed at this level but they must have direct access to give advice to senior managers who are making decisions about personal data processing.

What details do we have to publish about the DPO?

The GDPR requires you to:

- publish the contact details of your DPO; and
- provide them to the ICO.

This is to enable individuals, your employees and the ICO to contact the DPO as needed. You aren't required to include the name of the DPO when publishing their contact details but you can choose to provide this if you think it's necessary or helpful.

You're also required to provide your DPO's contact details in the following circumstances:

- when consulting the ICO under Article 36 about a DPIA; and
- when providing privacy information to individuals under Articles 13 and 14.

However, remember you do have to provide your DPO's name if you report a personal data breach to the ICO and to those individuals affected by it.

Is the DPO responsible for compliance?

The DPO isn't personally liable for data protection compliance. As the controller or processor it remains your responsibility to comply with the GDPR. Nevertheless, the DPO clearly plays a crucial role in helping you to fulfil your organisation's data protection obligations.

Further Reading

Relevant provisions in the GDPR - See Articles 35-36, 37-39, 83 and Recital 97
External link

In more detail - ICO guidance

See the following section of the Guide to GDPR: Accountability and governance

See our Guide to freedom of information

In more detail – Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The Article 29 Working Party has published guidelines on DPOs and DPO FAQs.

Codes of conduct and certification

At a glance

- The GDPR endorses the use of approved codes of conduct and certification mechanisms to demonstrate that you comply.
- The specific needs of micro, small and medium sized enterprises must be taken into account.
- Signing up to a code of conduct or certification scheme is not obligatory. But if an approved code of conduct or certification scheme that covers your processing activity becomes available, you may wish to consider working towards it as a way of demonstrating that you comply.
- Adhering to codes of conduct and certification schemes brings a number of benefits over and above demonstrating that you comply. It can:
  - improve transparency and accountability - enabling individuals to distinguish the organisations that meet the requirements of the law and they can trust with their personal data.
  - provide mitigation against enforcement action; and
  - improve standards by establishing best practice.
- When contracting work to third parties, including processors, you may wish to consider whether they have signed up to codes of conduct or certification mechanisms.

In brief

Who is responsible for drawing up codes of conduct?

- Governments and regulators can **encourage** the drawing up of codes of conduct.
- Codes of conduct may be created by trade associations or representative bodies.
- Codes should be prepared in consultation with relevant stakeholders, including individuals (Recital 99).
- Codes must be approved by the relevant supervisory authority; and where the processing is cross-border, the European Data Protection Board (the EDPB).
- Existing codes can be amended or extended to comply with the requirements under the GDPR.

What will codes of conduct address?

Codes of conduct should help you comply with the law, and may cover topics such as:

- fair and transparent processing;
- legitimate interests pursued by controllers in specific contexts;
- the collection of personal data;
- the pseudonymisation of personal data;
- the information provided to individuals and the exercise of individuals' rights;
- the information provided to and the protection of children (including mechanisms for obtaining

parental consent);

- technical and organisational measures, including data protection by design and by default and security measures;
- breach notification;
- data transfers outside the EU; or
- dispute resolution procedures.

What are the practical implications?

If you sign up to a code of conduct, you will be subject to mandatory monitoring by a body accredited by the supervisory authority.

If you infringe the requirements of the code of practice, you may be suspended or excluded and the supervisory authority will be informed. You also risk being subject to a fine of up to 10 million Euros or 2 per cent of your global turnover.

Adherence to a code of conduct may serve as a mitigating factor when a supervisory authority is considering enforcement action via an administrative fine.

Who is responsible for certification mechanisms?

Member states, supervisory authorities, the EDPB or the Commission are required to encourage the establishment of certification mechanisms to enhance transparency and compliance with the Regulation.

Certification will be issued by supervisory authorities or accredited certification bodies.

What is the purpose of a certification mechanism?

A certification mechanism is a way of you demonstrating that you comply, in particular, showing that you are implementing technical and organisational measures.

A certification mechanism may also be established to demonstrate the existence of appropriate safeguards related to the adequacy of data transfers.

They are intended to allow individuals to quickly assess the level of data protection of a particular product or service.

What are the practical implications?

Certification does not reduce your data protection responsibilities.

You must provide all the necessary information and access to your processing activities to the certification body to enable it to conduct the certification procedure.

Any certification will be valid for a maximum of three years. It can be withdrawn if you no longer meet the requirements of the certification, and the supervisory authority will be notified.

If you fail to adhere to the standards of the certification scheme, you risk being subject to an administrative fine of up to 10 million Euros or 2 per cent of your global turnover.

Further Reading

Relevant provisions in the GDPR - see Articles 40-43 and 83 and Recitals 98, 99, 100, 148, 150 and 151

External link

Article 29 Working Party

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The Article 29 Working Party now expects that guidelines on certification will be adopted in early 2018.

The Article 29 Working Party has adopted guidelines on imposing administrative fines.

Guide to the data protection fee

The Government has announced a new charging structure for data controllers to ensure the continued funding of the Information Commissioner's Office (ICO).

The new structure was laid before Parliament as a Statutory Instrument and will come into effect on 25 May 2018, to coincide with the General Data Protection Regulation.

Until then, organisations are legally required to pay the current notification fee, unless they are exempt.

To help data controllers understand why there's a new funding model and what they'll be required to pay from 25 May 2018, the ICO has produced a Guide to the Data Protection Fee.

The model must still be approved by Parliament before it is finally confirmed. But our guide reflects the draft and is intended to help data controllers prepare for what Government is proposing.

Further Reading

The data protection fee - a guide for controllers

For organisations
PDF (207.19K)

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.

Checklists

☐ 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 such as those specified by established frameworks like Cyber Essentials.

☐ 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.

In brief

- What's new?
- What does the GDPR say about security?
- Why should we worry about information security?
- What do we need to protect with our security measures?
- What level of security is required?
- What organisational measures do we need to consider?
- What technical measures do we need to consider?
- What if we operate in a sector that has its own security requirements?
- What do we do when a data processor is involved?
- What are 'confidentiality, integrity, availability' and 'resilience'?
- What are the requirements for restoring availability and access to personal data?
- Are we required to ensure our security measures are effective?
- What about codes of conduct and certification?
- What about our staff?

What's new?

The GDPR requires you to process personal data securely. This is not a new data protection obligation. It replaces and mirrors the previous requirement to have 'appropriate technical and organisational measures' under the Data Protection Act 1998 (the 1998 Act).

However, 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. Whilst these are broadly equivalent to what was considered good and best practice under the 1998 Act, they are now a legal requirement.

What does the GDPR say about security?

Article 5(1)(f) of the GDPR concerns the 'integrity and confidentiality' of personal data. It says that personal data shall be:

> 'Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'

You can refer to this as the GDPR's 'security principle'. It concerns the broad concept of **information security**.

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.

You need to consider the security principle alongside Article 32 of the GDPR, which provides more specifics on the security of your processing. Article 32(1) states:

> 'Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk'

Further Reading

Relevant provisions in the GDPR - See Articles 5(1)(f) and 32, and Recitals 39 and 83
External link

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.

The ICO is also required to consider the technical and organisational measures you had in place when considering an administrative fine.

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 (and that those people only act within the scope of the authority you give them);
- the data you hold is accurate and complete in relation to why you are processing it; and
- the data remains accessible and usable, ie, 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.

This reflects both the GDPR’s risk-based approach, and 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.

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. You should also take account of factors such as:

- the nature and extent of your organisation’s premises and computer systems;
- the number of staff you have and the extent of their access to personal data; and
- any personal data held or used by a data processor acting on your behalf.

Further Reading

Relevant provisions in the GDPR - See See Article 32(2) and Recital 83
External link

We cannot provide a complete guide to all aspects of security in all circumstances for all organisations, but this guidance is intended to identify the main points for you to consider.

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.

Example

The Chief Executive of a medium-sized organisation asks the Director of Resources to ensure that appropriate security measures are in place, and that regular reports are made to the board.

The Resources Department takes responsibility for designing and implementing the organisation's security policy, writing procedures for staff to follow, organising staff training, checking whether security measures are actually being adhered to and investigating security incidents.

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.

Whether or not you have such a policy, you still need to consider security and other related matters such as:

- co-ordination between key people in your organisation (eg the security manager will need to know about commissioning and disposing of any IT equipment);
- access to premises or equipment given to anyone outside your organisation (eg for computer maintenance) and the additional security considerations this will generate;
- business continuity arrangements that identify how you will protect and recover any personal data you hold; and
- periodic checks to ensure that your security measures remain appropriate and up to date.

What technical measures do we need to consider?

Technical measures are sometimes thought of as the protection of personal data held in computers and networks. Whilst these are of obvious importance, many security incidents can be due to the theft or loss of equipment, the abandonment of old computers or hard-copy records being lost, stolen or incorrectly disposed of. Technical measures therefore include both physical and computer or IT security.

When considering physical security, you should look at factors such as:

- the quality of doors and locks, and the protection of your premises by such means as alarms, security lighting or CCTV;
- how you control access to your premises, and how visitors are supervised;
- how you dispose of any paper and electronic waste; and
- how you keep IT equipment, particularly mobile devices, secure.

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.

When considering cybersecurity, you should look at factors such as:

- system security – the security of your network and information systems, including those which process personal data;
- data security – the security of the data you hold within your systems, eg ensuring appropriate access controls are in place and that data is held securely;
- online security – eg the security of your website and any other online service or application that you use; and
- device security – including policies on Bring-your-own-Device (BYOD) if you offer it.

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.

Whatever you do, you should remember the following:

- your cybersecurity measures need to be appropriate to the size and use of your network and information systems;
- you should take into account the state of technological development, but you are also able to consider the costs of implementation;
- your security must be appropriate to your business practices. For example, if you offer staff the ability to work from home, you need to put measures in place to ensure that this does not compromise your security; and
- your measures must be appropriate to the nature of the personal data you hold and the harm that might result from any compromise.

A good starting point is to make sure that you're in line with the requirements of Cyber Essentials – a government scheme that includes a set of basic technical controls you can put in place relatively easily.

You should however be aware that you may have to go beyond these requirements, depending on your processing activities. Cyber Essentials is only intended to provide a 'base' set of controls, and won't

address the circumstances of every organisation or the risks posed by every processing operation.

A list of helpful sources of information about cybersecurity is provided below.

Other resources

The Cyber Essentials scheme

In more detail – ICO guidance

Under the 1998 Act, the ICO published a number of more detailed guidance pieces on different aspects of IT security. We will be updating each of these to reflect the GDPR's requirements in due course. However, until that time they may still provide you with assistance or things to consider.

- IT security top tips – for further general information on IT security;
- IT asset disposal for organisations (pdf) – guidance to help organisations securely dispose of old computers and other IT equipment;
- A practical guide to IT security – ideal for the small business (pdf);
- Protecting personal data in online services – learning from the mistakes of others (pdf) – detailed technical guidance on common technical errors the ICO has seen in its casework
- Bring your own device (BYOD) (pdf) – guidance for organisations who want to allow staff to use personal devices to process personal data;
- Cloud computing (pdf) – guidance covering how security requirements apply to personal data processed in the cloud; and
- Encryption – advice on the use of encryption to protect personal data.

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, the ICO will nevertheless consider these carefully in any considerations of regulatory action. It can be the case that they specify certain measures that you should have, and that those measures contribute to your overall security posture.

Example

If you are processing payment card data, you are obliged to comply with the Payment Card Industry Data Security Standard. The PCI-DSS outlines a number of specific technical and

organisational measures that the payment card industry considers applicable whenever such data is being processed.

Although compliance with the PCI-DSS is not necessarily equivalent to compliance with the GDPR's security principle, if you process card data and suffer a personal data breach, the ICO will consider the extent to which you have put in place measures that PCI-DSS requires particularly if the breach related to a lack of a particular control or process mandated by the standard.

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 stipulate that the processor takes all measures required under Article 32 – basically, the contract has to 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 for 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.

Further Reading

Relevant provisions in the GDPR - See Articles 28 and 32, and Recitals 81 and 83
External link

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.

However, there are a wide range of solutions that allow you to implement both without great cost or difficulty. For example, for a number of years the ICO has considered encryption to be an appropriate technical measure given its widespread availability and relatively low cost of implementation. This position has not altered due to the GDPR — if you are storing personal data, or transmitting it over the internet, we recommend that you use encryption and have a suitable policy in place, taking account of

the residual risks involved.

When considering what to put in place, you should undertake a risk analysis and document your findings.

Further Reading

Relevant provisions in the GDPR - See Article 32(1)(a) and Recital 83
External link

In more detail – ICO guidance

We have published detailed guidance on encryption under the 1998 Act. Much of this guidance still applies, however we are also working to update it to reflect the GDPR.

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.

Further Reading

Relevant provisions in the GDPR - See Article 32(1)(b) and Recital 83
External link

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.

Example

An organisation takes regular backups of its systems and the personal data held within them. It follows the well-known '3-2-1' backup strategy: three copies, with two stored on different devices and one stored off-site.

The organisation is targeted by a ransomware attack that results in the data being encrypted. This means that it is no longer able to access the personal data it holds.

Depending on the nature of the organisation and the data it processes, this lack of availability can have significant consequences on individuals – and would therefore be a personal data breach under the GDPR.

The ransomware has spread throughout the organisation's systems, meaning that two of the backups are also unavailable. However, the third backup, being stored off-site, allows the organisation to restore its systems in a timely manner. There may still be a loss of personal data depending on when the off-site backup was taken, but having the ability to restore the systems means that whilst there will be some disruption to the service, the organisation are nevertheless able to comply with this requirement of the GDPR.

Further Reading

Relevant provisions in the GDPR - See Article 32(1)(c) and Recital 83
External link

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 essentially '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 testing internally or externally. In some cases it is recommended that both take place.

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.

Further Reading

Relevant provisions in the GDPR - See Article 32(1)(d) and Recital 83
External link

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.

Further Reading

Relevant provisions in the GDPR - See Article 32(3) and Recital 83
External link

In more detail - Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The Article 29 Working Party will be producing specific guidance on certification in the coming months.

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 the 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 (eg 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 (eg to avoid virus infection or spam).

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

Further Reading

Relevant provisions in the GDPR - See Article 32(4) and Recital 83
External link

Other resources

The NCSC has detailed technical guidance in a number of areas that will be relevant to you whenever you process personal data. Some examples include:

- 10 Steps to Cyber Security – The 10 Steps define and communicate an Information Risk Management Regime which can provide protection against cyber-attacks.
- The Cyber Essentials scheme – this provides a set of basic technical controls that you can implement to guard against common cyber threats.
- Risk management collection – a collection of guidance on how to assess cyber risk.

The government has produced relevant guidance on cybersecurity:

- CyberAware – a cross-government awareness campaign developed by the Home Office, the Department for Digital, Culture, Media and Sport ('DCMS') and the NCSC.
- 'Cybersecurity – what small businesses need to know' – produced by DCMS and the department for Business, Enterprise, Innovation and Skills ('BEIS').

Technical guidance produced by the European Union Agency for Network and Information Security (ENISA) may also assist you:

- Data protection section at ENISA's website

International transfers

At a glance

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

In brief

When can personal data be transferred outside the European Union?

Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

What about transfers on the basis of a Commission decision?

Transfers may be made where the Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.

Further Reading

Relevant provisions in the GDPR - see Article 45 and Recitals 103-107 and 169
External link

What about transfers subject to appropriate safeguards?

You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

Adequate safeguards may be provided for by:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- compliance with an approved code of conduct approved by a supervisory authority;
- certification under an approved certification mechanism as provided for in the GDPR;

- contractual clauses agreed authorised by the competent supervisory authority; or
- provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

Further Reading

Relevant provisions in the GDPR - see Article 46 and Recitals 108-110 and 114
External link

Article 29 Working Party

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

According to its workplan, the Article 29 Working Party will publish guidelines on data transfers based on binding corporate rules and contractual clauses in 2017.

What about transfers based on an organisation's assessment of the adequacy of protection?

The GDPR limits your ability to transfer personal data outside the EU where this is based only on your own assessment of the adequacy of the protection afforded to the personal data.

Authorisations of transfers made by Member States or supervisory authorities and decisions of the Commission regarding adequate safeguards made under the Directive will remain valid/remain in force until amended, replaced or repealed.

Further Reading

Relevant provisions in the GDPR - see Articles 83 and 84 and Recitals 148-152
External link

Are there any derogations from the prohibition on transfers of personal data outside of the EU?

The GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations. A transfer, or set of transfers, may be made where the transfer is:

- made with the individual's informed consent;
- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- necessary for important reasons of public interest;
- necessary for the establishment, exercise or defence of legal claims;

- necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

The first three derogations are not available for the activities of public authorities in the exercise of their public powers.

Further Reading

Relevant provisions in the GDPR - see Article 49 and Recitals 111 and 112
External link

What about one-off (or infrequent) transfers of personal data concerning only relatively few individuals?

Even where there is no Commission decision authorising transfers to the country in question, if it is not possible to demonstrate that individual's rights are protected by adequate safeguards and none of the derogations apply, the GDPR provides that personal data may still be transferred outside the EU.

However, such transfers are permitted only where the transfer:

- is not being made by a public authority in the exercise of its public powers;
- is not repetitive (similar transfers are not made on a regular basis);
- involves data related to only a limited number of individuals;
- is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual); and
- is made subject to suitable safeguards put in place by the organisation (in the light of an assessment of all the circumstances surrounding the transfer) to protect the personal data.

In these cases, organisations are obliged to inform the relevant supervisory authority of the transfer and provide additional information to individuals.

Further Reading

Relevant provisions in the GDPR - see Article 49 and Recital 113
External link

Further reading

Blog: Changes to Binding Corporate Rules applications to the ICO
External link

Personal data breaches

At a glance

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Checklists

Preparing for a personal data breach

☐ We know how to recognise a personal data breach.

☐ We understand that a personal data breach isn't only about loss or theft of personal data.

☐ We have prepared a response plan for addressing any personal data breaches that occur.

☐ We have allocated responsibility for managing breaches to a dedicated person or team.

☐ Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Responding to a personal data breach

☐ We have in place a process to assess the likely risk to individuals as a result of a breach.

☐ We know who is the relevant supervisory authority for our processing activities.

☐ We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.

☐ We know what information we must give the ICO about a breach.

☐ We have a process to inform affected individuals about a breach when it is likely to result in a

high risk to their rights and freedoms.

☐ We know we must inform affected individuals without undue delay.

☐ We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.

☐ We document all breaches, even if they don't all need to be reported.

In brief

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Example

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify

the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

> "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

Example

The theft of a customer database, the data of which may be used to commit identity fraud, would need to be notified, given the impact this is likely to have on those individuals who could suffer financial loss or other consequences. On the other hand, you would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of a staff telephone list.

So, on becoming aware of a breach, you should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

For more details about assessing risk, please see section IV of the Article 29 Working Party guidelines on personal data breach notification.

What role do processors have?

If your organisation uses a data processor, and this processor suffers a breach, then under Article 33(2) it must inform you without undue delay as soon as it becomes aware.

Example

Your organisation (the controller) contracts an IT services firm (the processor) to archive and store

customer records. The IT firm detects an attack on its network that results in personal data about its clients being unlawfully accessed. As this is a personal data breach, the IT firm promptly notifies you that the breach has taken place. You in turn notify the ICO.

This requirement allows you to take steps to address the breach and meet your breach-reporting obligations under the GDPR.

If you use a processor, the requirements on breach reporting should be detailed in the contract between you and your processor, as required under Article 28. For more details about contracts, please see our draft GDPR guidance on contracts and liabilities between controllers and processors.

How much time do we have to report a breach?

You must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

Section II of the Article 29 Working Party Guidelines on personal data breach notification gives more details of when a controller can be considered to have "become aware" of a breach.

What information must a breach notification to the supervisory authority contain?

When reporting a breach, the GDPR says you must provide:

- a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

What if we don't have all the required information available yet?

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So Article 34(4) allows you to provide the required information in phases, as long as this is done without undue further delay.

However, we expect controllers to prioritise the investigation, give it adequate resources, and expedite it urgently. You must still notify us of the breach when you become aware of it, and submit further information as soon as possible. If you know you won't be able to provide full details within 72 hours, it is a good idea to explain the delay to us and tell us when you expect to submit more information.

Example

You detect an intrusion into your network and become aware that files containing personal data have been accessed, but you don't know how the attacker gained entry, to what extent that data was accessed, or whether the attacker also copied the data from your system.

You notify the ICO within 72 hours of becoming aware of the breach, explaining that you don't yet have all the relevant details, but that you expect to have the results of your investigation within a few days. Once your investigation uncovers details about the incident, you give the ICO more information about the breach without delay.

How do we notify a breach to the ICO?

To notify the ICO of a personal data breach, please see our pages on reporting a breach.

Remember, in the case of a breach affecting individuals in different EU countries, the ICO may not be the lead supervisory authority. This means that as part of your breach response plan, you should establish which European data protection agency would be your lead supervisory authority for the processing activities that have been subject to the breach. For more guidance on determining who your lead authority is, please see the Article 29 Working Party guidance on identifying your lead authority.

When do we need to tell individuals about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Again, you will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

Example

A hospital suffers a breach that results in an accidental disclosure of patient records. There is likely to be a significant impact on the affected individuals because of the sensitivity of the data and their confidential medical details becoming known to others. This is likely to result in a high risk to their rights and freedoms, so they would need to be informed about the breach.

A university experiences a breach when a member of staff accidentally deletes a record of alumni contact details. The details are later re-created from a backup. This is unlikely to result in a high risk to the rights and freedoms of those individuals. They don't need to be informed about the breach.

If you decide not to notify individuals, you will still need to notify the ICO unless you can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. You should also remember that the

ICO has the power to compel you to inform affected individuals if we consider there is a high risk. In any event, you should document your decision-making process in line with the requirements of the accountability principle.

What information must we provide to individuals when telling them about a breach?

You need to describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of your data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Does the GDPR require us to take any other steps in response to a breach?

You should ensure that you record all breaches, regardless of whether or not they need to be reported to the ICO.

Article 33(5) requires you to document the facts relating to the breach, its effects and the remedial action taken. This is part of your overall obligation to comply with the accountability principle, and allows us to verify your organisation's compliance with its notification duties under the GDPR.

As with any security incident, you should investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

What else should we take into account?

The following aren't specific GDPR requirements, but you may need to take them into account when you've experienced a breach.

It is important to be aware that you may have additional notification obligations under other laws if you experience a personal data breach. For example:

- If you are a communications service provider, you must notify the ICO of any personal data breach within 24 hours under the Privacy and Electronic Communications Regulations (PECR). You should use our PECR breach notification form, rather than the GDPR process. Please see our pages on PECR for more details.
- If you are a UK trust service provider, you must notify the ICO of a security breach, which may include a personal data breach, within 24 hours under the Electronic Identification and Trust Services (eIDAS) Regulation. Where this includes a personal data breach you can use our eIDAS breach notification form or the GDPR breach-reporting process. However, if you report it to us under the GDPR, this still must be done within 24 hours. Please read our Guide to eIDAS for more information.
- If your organisation is an operator of essential services or a digital service provider, you will have incident-reporting obligations under the NIS Directive. These are separate from personal data breach notification under the GDPR. If you suffer an incident that's also a personal data breach, you will still need to report it to the ICO separately, and you should use the GDPR process for doing so.

You may also need to consider notifying third parties such as the police, insurers, professional bodies, or

bank or credit card companies who can help reduce the risk of financial loss to individuals.

The European Data Protection Board, which will replace the Article 29 Working Party, may issue guidelines, recommendations and best practice advice that may include further guidance on personal data breaches. You should look out for any such future guidance. Likewise, you should be aware of any recommendations issued under relevant codes of conduct or sector-specific requirements that your organisation may be subject to.

What happens if we fail to notify?

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of your global turnover. The fine can be combined the ICO's other corrective powers under Article 58. So it's important to make sure you have a robust breach-reporting process in place to ensure you detect and can notify a breach, on time; and to provide the necessary details.

Further Reading

Relevant provisions in the GDPR - See Articles 33, 34, 58, 83 and Recitals 75, 85-88
External link

In more detail - ICO guidance

See the following sections of the Guide to the GDPR:

- Security
- Accountability and governance

GDPR 'in more detail' guidance:

- Draft GDPR guidance on contracts and liabilities between controllers and processors

Existing DPA guidance:

- Encryption
- A practical guide to IT security: ideal for the small business

Other related guidance:

- Guide to PECR
- Notification of PECR security breaches
- Guide to eIDAS

In more detail - Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

Following the consultation period, the Article 29 Working Party has adopted final guidelines on personal data breach notification.

The Article 29 Working Party has published guidelines on lead supervisory authorities and lead supervisory authority FAQs.

Other resources

Report a security breach
For organisations

Exemptions

What derogations does the GDPR permit?

Article 23 enables Member States to introduce derogations to the GDPR in certain situations.

Member States can introduce exemptions from the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences;
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- the protection of judicial independence and proceedings;
- breaches of ethics in regulated professions;
- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- the protection of the individual, or the rights and freedoms of others; or
- the enforcement of civil law matters.

What about other Member State derogations or exemptions?

Chapter IX provides that Member States can provide exemptions, derogations, conditions or rules in relation to specific processing activities. These include processing that relates to:

- freedom of expression and freedom of information;
- public access to official documents;
- national identification numbers;
- processing of employee data;
- processing for archiving purposes and for scientific or historical research and statistical purposes;
- secrecy obligations; and
- churches and religious associations.

Further Reading

Relevant provisions in the GDPR - see Articles 6(2), 6(3), 9(a)(a), 23 and 85-91 and Recitals 71, 50, 53 and 153-165

External link

Applications

To assist organisations in applying the requirements of the GDPR in different contexts, we are working to produce guidance in a number of areas. For example, children’s data, CCTV, big data, etc.

This section will expand when our work on this guidance is complete.

Children

At a glance

- Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.
- If you process children's personal data then you should think about the need to protect them from the outset, and design your systems and processes with this in mind.
- Compliance with the data protection principles and in particular fairness should be central to all your processing of children's personal data.
- You need to have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child.
- If you are relying on consent as your lawful basis for processing personal data, when offering an online service directly to a child, only children aged 13 or over are able provide their own consent.(This is the age proposed in the Data Protection Bill and is subject to Parliamentary approval).
- For children under this age you need to get consent from whoever holds parental responsibility for the child - unless the online service you offer is a preventive or counselling service.
- Children merit specific protection when you use their personal data for marketing purposes or creating personality or user profiles.
- You should not usually make decisions based solely on automated processing about children if this will have a legal or similarly significant effect on them.
- You should write clear privacy notices for children so that they are able to understand what will happen to their personal data, and what rights they have.
- Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.
- An individual's right to erasure is particularly relevant if they gave their consent to processing when they were a child.

Checklists

General

☐ We comply with all the requirements of the GDPR, not just those specifically relating to children and included in this checklist.

☐ We design our processing with children in mind from the outset, and use a data protection by design and by default approach.

☐ We make sure that our processing is fair and complies with the data protection principles.

☐ As a matter of good practice, we use DPIAs to help us assess and mitigate the risks to

children.

☐ If our processing is likely to result in a high risk to the rights and freedom of children then we always do a DPIA.

☐ As a matter of good practice, we consult with children as appropriate when designing our processing.

Bases for processing a child's personal data

☐ When relying on consent, we make sure that the child understands what they are consenting to, and we do not exploit any imbalance in power in the relationship between us.

☐ When relying on 'necessary for the performance of a contract', we consider the child's competence to understand what they are agreeing to, and to enter into a contract.

☐ When relying upon 'legitimate interests', we take responsibility for identifying the risks and consequences of the processing, and put age appropriate safeguards in place.

Offering an information Society Service (ISS) directly to a child, on the basis of consent

☐ If we decide not to offer our ISS (online service) directly to children, then we mitigate the risk of them gaining access, using measures that are proportionate to the risks inherent in the processing.

☐ When offering ISS to UK children on the basis of consent, we make reasonable efforts (taking into account the available technology and the risks inherent in the processing) to ensure that anyone who provides their own consent is at least 13 years old.

☐ When offering ISS to UK children on the basis of consent, we obtain parental consent to the processing for children who are under the age of 13, and make reasonable efforts (taking into account the available technology and risks inherent in the processing) to verify that the person providing consent holds parental responsibility for the child.

☐ When targeting wider European markets we comply with the age limits applicable in each Member state.

☐ We regularly review available age verification and parental responsibility verification mechanisms to ensure we are using appropriate current technology to reduce risk in the processing of children's personal data.

☐ We don't seek parental consent when offering online preventive or counselling services to a child.

Marketing

☐ When considering marketing children we take into account their reduced ability to recognise and critically assess the purposes behind the processing and the potential consequences of providing their personal data.

☐ We take into account sector specific guidance on marketing, such as that issued by the Advertising Standards Authority, to make sure that children's personal data is not used in a way that might lead to their exploitation.

☐ We stop processing a child's personal data for the purposes of direct marketing if they ask us to.

☐ We comply with the direct marketing requirements of the Privacy and Electronic Communications Regulations (PECR).

Solely automated decision making (including profiling)

☐ We don't usually use children's personal data to make solely automated decisions about them if these will have a legal, or similarly significant effect upon them.

☐ If we do use children's personal data to make such decisions then we make sure that one of the exceptions in Article 22(2) applies and that suitable, child appropriate, measures are in place to safeguard the child's rights, freedoms and legitimate interests.

☐ In the context of behavioural advertising, when deciding whether a solely automated decision has a similarly significant effect upon a child, we take into account: the choices and behaviours that we are seeking to influence; the way in which these might affect the child; and the child's increased vulnerability to this form of advertising; using wider evidence on these matters to support our assessment.

☐ We stop any profiling of a child that is related to direct marketing if they ask us to.

Privacy notices

☐ Our privacy notices are clear, and written in plain, age-appropriate language.

☐ We use child friendly ways of presenting privacy information, such as: diagrams, cartoons, graphics and videos, dashboards, layered and just-in-time notices, icons and symbols.

☐ We explain to children why we require the personal data we have asked for, and what we will do with it, in a way which they can understand.

☐ As a matter of good practice, we explain the risks inherent in the processing, and how we intend to safeguard against them, in a child friendly way, so that children (and their parents) understand the implications of sharing their personal data.

☐ We tell children what rights they have over their personal data in language they can understand.

☐ As a matter of good practice, if we are relying upon parental consent then we offer two different versions of our privacy notices; one aimed at the holder of parental responsibility and one aimed at the child.

The child's data protection rights

☐ We design the processes by which a child can exercise their data protection rights with the child in mind, and make them easy for children to access and understand.

☐ We allow competent children to exercise their own data protection rights.

☐ If our original processing was based on consent provided when the individual was a child, then we comply with requests for erasure whenever we can.

☐ We design our processes so that, as far as possible, it is as easy for a child to get their personal data erased as it was for them to provide it in the first place.

In brief

- What's new?
- What should our general approach to processing children's personal data be?
- What do we need to think about when choosing a basis for processing children's personal data?
- What are the rules about an ISS and consent?
- What if we want to market to Children?
- What if we want to profile children or make automated decisions about them?
- How does the right to be informed apply to children?
- How does the right to erasure apply to children?

What's new?

A child's personal data merits particular protection under the GDPR.

If you rely on consent as your lawful basis for processing personal data when offering an ISS directly to children, only children aged 13 or over are able provide their own consent. You may therefore need to verify that anyone giving their own consent in these circumstances is old enough to do so.

For children under this age you need to get consent from whoever holds parental responsibility for them - unless the ISS you offer is an online preventive or counselling service.

You must make reasonable efforts (using available technology) to verify that the person giving consent does, in fact, hold parental responsibility for the child.

Children merit specific protection when you are collecting their personal data and using it for marketing purposes or creating personality or user profiles.

You should not usually make decisions about children based solely on automated processing if this will have a legal or similarly significant effect on them. The circumstances in which the GDPR allows you to make such decisions are limited and only apply if you have suitable measures to protect the interests of the child in place.

You must write clear and age-appropriate privacy notices for children.

The right to have personal data erased is particularly relevant when the individual gave their consent to processing when they were a child.

What should our general approach to processing children's personal data be?

Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.

If you process children's personal data, or think that you might, then you should consider the need to protect them from the outset, and design your systems and processes with this in mind.

Fairness, and compliance with the data protection principles, should be central to all your processing of children's personal data.

It is good practice to consult with children when designing your processing.

What do we need to think about when choosing a basis for processing children's personal data?

As with adults, you need to have a lawful basis for processing a child's personal data and you need to decide what that basis is before you start processing.

You can use any of the lawful bases for processing set out in the GDPR when processing children's personal data. But for some bases there are additional things you need to think about when your data subject is a child.

If you wish to rely upon consent as your lawful basis for processing, then you need to ensure that the child can understand what they are consenting to, otherwise the consent is not 'informed' and therefore invalid. There are also some additional rules for online consent.

If you wish to rely upon 'performance of a contract' as your lawful basis for processing, then you must consider the child's competence to agree to the contract and to understand the implications of this processing.

If you wish to rely upon legitimate interests as your lawful basis for processing you must balance your own (or a third party's) legitimate interests in processing the personal data against the interests and fundamental rights and freedoms of the child. This involves a judgement as to the nature and purpose of the processing and the potential risks it poses to children. It also requires you to take appropriate measures to safeguard against those risks.

What are the rules about an ISS and consent?

Consent is not the only basis for processing children's personal data in the context of an ISS.

However, if you do rely upon consent as your lawful basis for processing personal data when offering an ISS directly to children, in the UK only children aged 13 or over can consent for themselves. (This is the age proposed in the Data Protection Bill and is subject to Parliamentary approval). You therefore need to make reasonable efforts to verify that anyone giving their own consent in this context is old enough to do so.

For children under this age you need to get consent from whoever holds parental responsibility for them - unless the ISS you offer is an online preventive or counselling service.

You must make reasonable efforts (using available technology) to verify that the person giving consent does, in fact, hold parental responsibility for the child.

You should regularly review the steps you are taking to protect children's personal data and consider whether you are able to implement more effective verification mechanisms when obtaining consent for processing.

What if we want to market to children?

Children merit specific protection when you are using their personal data for marketing purposes. You should not exploit any lack of understanding or vulnerability.

They have the same right as adults to object to you processing their personal data for direct marketing. So you must stop doing this if a child (or someone acting on their behalf) asks you to do so.

If you wish to send electronic marketing messages to children then you also need to comply with the Privacy and Electronic Communications Regulations 2003.

What if we want to profile children or make automated decisions about them?

In most circumstances you should not make decisions about children that are based solely on automated processing, (including profiling) if these have a legal effect on the child, or similarly significantly affect them.

The GDPR gives children the right not to be subject to this type of decision. Although there are exceptions to this right, they only apply if suitable measures are in place to protect the rights, freedoms and legitimate interests of the child.

If you profile children then you must provide them with clear information about what you are doing with their personal data. You should not exploit any lack of understanding or vulnerability.

You should generally avoid profiling children for marketing purposes. You must respect a child's absolute right to object to profiling that is related to direct marketing, and stop doing this if they ask you to.

It is possible for behavioural advertising to 'similarly significantly affect' a child. It depends on the nature of the choices and behaviour it seeks to influence.

How does the right to be informed apply to children?

You must provide children with the same information about what you do with their personal data as you give adults. It is good practice to also explain the risks inherent in the processing and the safeguards you have put in place.

You should write in a concise, clear and plain style for any information you are directing to children. It should be age-appropriate and presented in a way that appeals to a young audience.

If you are relying upon parental consent as your lawful basis for processing it is good practice to provide

separate privacy notices aimed at both the child and the responsible adult.

If you provide an ISS and children younger than your target age range are likely to try and access it then it is good practice to explain any age limit to them in language they can understand.

Children have the same rights as adults over their personal data and can exercise their own rights as long as they are competent to do so. Where a child is not considered to be competent, an adult with parental responsibility may exercise the child's data protection rights on their behalf.

How does the right to erasure apply to children?

Children have the same right to have their personal data erased as adults.

This right is particularly relevant when an individual originally gave their consent to processing when they were a child, without being fully aware of the risks.

One of the specified circumstances in which the right to erasure applies is when you collected the personal data of a child under the lawful basis of consent, when offering an ISS directly to a child.

It should generally be as easy for a child to exercise their right to erasure as it was for them to provide their personal data in the first place.

Further Reading

Relevant provisions in the GDPR - See Articles 8, 12(1) and 17(1)(f) and Recitals 38, 58, 65, and 71

External link

In more detail - ICO guidance

We have published detailed guidance on Children and the GDPR for public consultation. The consultation closes on 28 February 2018.