Guide to the General Data Protection Regulation (GDPR)

ico.
Information Commissioner's Office

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

Getting ready for the GDPR checklist
For organisations

What's new

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

February 2018

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?

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. This is however a one-off opportunity to bring your processing in line with the GDPR. Once the GDPR is in effect, you will not be able 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 determine the appropriate lawful basis (or bases, if more than one applies) from the start.

The GDPR also 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:

	Right to erasure	**Right to portability**	**Right to object**
Consent	✓	✓	**X** but right to withdraw consent
Contract	✓	✓	**X**
Legal obligation	**X**	**X**	**X**
Vital interests	✓	**X**	**X**

Public task	X	X	✓
Legitimate interests	✓	X	✓

Note that not all of these rights are 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.

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, you cannot simply swap to a different one. Even if a different basis could have applied from the start, retrospectively switching lawful basis is likely to be inherently unfair to the individual and lead to breaches of accountability and transparency requirements.

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

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.

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. 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.

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 customer 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 individual ('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 is valid consent?
- How should you 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 individual ('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 consent (or explicit consent) can also legitimise use of special category data, restricted processing, automated decision-making and overseas transfers of data.

Genuine consent should put individuals in control, build customer 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 you 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 have analysed the feedback received to our draft consent guidance. A summary of the responses can be found on the Consultations pages of the website.

We will publish a final updated version of our guidance once the final content of the Article 29

Working Party guidelines is clear.

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 published guidelines on consent in December 2017. The period for public comment has ended. See the Article 29 website for more details.

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?

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

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?

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

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?

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

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?

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.

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 notice.

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 notice.

In brief

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 notice.

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 notice, 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 – and 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 it 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 notice 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 are planning to publish more detailed guidance on this topic shortly.

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?

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?

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

- The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice.
- It emphasises the need for transparency over how you use personal data.

In brief

What information must be supplied?

The GDPR sets out the information that you should supply and when individuals should be informed.

The information you supply is determined by whether or not you obtained the personal data directly from individuals. See the table below for further information on this.

The information you supply about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The table below summarises the information you should supply to individuals and at what stage.

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓

Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	✓	✓
When should information be provided?	At the time the data are obtained.	Within a reasonable period of having obtained the data (within one month)
		If the data are used to communicate with the individual, at the latest, when the first communication takes place; or
		If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

Further Reading

Relevant provisions in the GDPR - see Articles 12(1), 12(5), 12(7), 13 and 14 and Recitals 58-62
External link

In more detail - ICO guidance

Further guidance for organisations on how to comply with 'the right to be informed' is provided in the ICO privacy notices code of practice.

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 transparency. The consultation period for these guidelines has ended.

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 gives individuals the right to have personal data rectified.
- Personal data can be rectified if it is inaccurate or incomplete.

In brief

When should personal data be rectified?

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

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

How long do I have to comply with a request for rectification?

You must respond within one month.

This can be extended by two months where the request for rectification is complex.

Where you are not taking action in response to a request for rectification, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

Further Reading

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

Right to erasure

At a glance

- The right to erasure is also known as ‘the right to be forgotten’.
- The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

In brief

When does the right to erasure apply?

The right to erasure does not provide an absolute ‘right to be forgotten’. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Under the GDPR, this right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

There are some specific circumstances where the right to erasure does not apply and you can refuse to deal with a request.

When can I refuse to comply with a request for erasure?

You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

How does the right to erasure apply to children's personal data?

There are extra requirements when the request for erasure relates to children's personal data, reflecting the GDPR emphasis on the enhanced protection of such information, especially in online environments.

If you process the personal data of children, you should pay special attention to existing situations where a child has given consent to processing and they later request erasure of the data (regardless of age at the time of the request), especially on social networking sites and internet forums. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent (Recital 65).

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

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

The GDPR reinforces the right to erasure by clarifying that organisations in the online environment who make personal data public should inform other organisations who process the personal data to erase links to, copies or replication of the personal data in question.

While this might be challenging, if you process personal information online, for example on social networks, forums or websites, you must endeavour to comply with these requirements.

As in the example below, there may be instances where organisations that process the personal data may not be required to comply with this provision because an exemption applies.

Example

A search engine notifies a media publisher that it is delisting search results linking to a news report as a result of a request for erasure from an individual. If the publication of the article is protected by the freedom of expression exemption, then the publisher is not required to erase the article.

Further Reading

Relevant provisions in the GDPR - see Articles 17 and 19 and Recitals 65 and 66
External link

Right to restrict processing

At a glance

- Individuals have a right to 'block' or suppress processing of personal data.
- When processing is restricted, you are permitted to store the personal data, but not further process it.
- You can retain just enough information about the individual to ensure that the restriction is respected in future.

In brief

When does the right to restrict processing apply?

You will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

You may need to review procedures to ensure you are able to determine where you may be required to restrict the processing of personal data.

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

You must inform individuals when you decide to lift a restriction on processing.

Further Reading

Relevant provisions in the GDPR - see Articles 18 and 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 hindrance to usability.
- Some organisations in the UK already offer data portability through the 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.
- It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

Example

midata is used to improve transparency across the banking industry by providing personal current account customers access to their transactional data for their account(s), which they can upload to a third party price comparison website to compare and identify best value. A price comparison website displays alternative current account providers based on their own calculations.

In brief

When does the right to data portability apply?

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

How do I comply?

You must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The information must be provided free of charge.

If the individual requests it, you may be required to transmit the data directly to another organisation if this is technically feasible. However, you are not required to adopt or maintain processing systems that are technically compatible with other organisations.

If the personal data concerns more than one individual, you must consider whether providing the information would prejudice the rights of any other individual.

How long do I have to comply?

You must respond without undue delay, and within one month.

This can be extended by two months where the request is complex or you receive a number of requests. You must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where you are not taking action in response 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.

Further Reading

Relevant provisions in the GDPR - see Articles 12 and 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?

- 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.

The Article 29 Working Party has published guidelines on Automated individual decision-making and Profiling. These were subject to a consultation process and the final version is due to be adopted in February 2018.

Other relevant guidelines published by WP29 include:

WP29 guidelines on consent

WP29 guidelines on Data Protection Impact Assessment

WP29 guidelines on transparency

Accountability and governance

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance.

You are expected to put into place comprehensive but proportionate governance measures. Good practice tools that the ICO has championed for a long time such as privacy impact assessments and privacy by design are now legally required in certain circumstances.

Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many organisations will already have good governance measures in place.

What is the accountability principle?

The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

How can I demonstrate that I comply?

You must:

- implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies;
- maintain relevant documentation on processing activities;
- where appropriate, appoint a data protection officer;
- implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
  - data minimisation;
  - pseudonymisation;
  - transparency;
  - allowing individuals to monitor processing; and
  - creating and improving security features on an ongoing basis.
- use data protection impact assessments where appropriate.

You can also:

- adhere to approved codes of conduct and/or certification schemes. See the section on codes of conduct and certification for more detail.

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?

- 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 less 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.

Please note

The Article 29 Working Party (WP29) is currently considering the scope of the exemption from documentation of processing activities for small and medium-sized organisations.

WP29 includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

If necessary, we will update this guidance to reflect the outcome of WP29's discussions.

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 (34.33K)

Documentation template for processors
For organisations
File (17.96K)

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

There are no immediate plans for WP29 guidance on documentation of processing activities under the GDPR, but WP29 is currently considering the scope of the exemption from documentation of processing activities for small and medium-sized organisations.

If necessary, we will update this guidance to reflect the outcome of WP29's discussions.

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

- Data protection impact assessments (DPIAs) help organisations to identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.
- DPIAs can be an integral part of taking a privacy by design approach.
- The GDPR sets out the circumstances in which a DPIA must be carried out.

In brief

What is a data protection impact assessment?

Data protection impact assessments (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

The ICO has promoted the use of DPIAs as an integral part of taking a privacy by design approach.

See the ICO's conducting privacy impact assessments code of practice for good practice advice. 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.

Annex 1 of the ICO's paper on big data, artificial intelligence, machine learning and data protection contains practical advice on applying GDPR DPIA provisions in the specific context of big data analytics.

When do I need to conduct a DPIA?

You must carry out a DPIA when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.
- large scale processing of special categories of data or personal data relation to criminal convictions or offences.

  This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms eg based on the sensitivity of the processing activity.
- large scale, systematic monitoring of public areas (CCTV).

What information should the DPIA contain?

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.
- A DPIA can address more than one project.

Further Reading

Relevant provisions in the GDPR - see Articles 35, 36 and 83 and Recitals 84 and 89-96
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 finalised its guidelines on high risk processing and DPIAs, following its consultation.

In more detail – ICO guidance

We are currently considering whether the ICO can provide any further detail over and above the Article 29 Working Party guidelines. We will add any additional advice we are able to provide here in due course.

Data protection officers

At a glance

- The GDPR makes it a requirement that organisations appoint a data protection officer (DPO) in some circumstances.
- The GDPR also contains provisions about the tasks a DPO should carry out and the duties of the employer in respect of the DPO.

In brief

When does a Data Protection Officer need to be appointed under the GDPR?

Under the GDPR, you **must** appoint a DPO if you:

- are a public authority (except for courts acting in their judicial capacity);
- carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

You may appoint a single data protection officer to act for a group of companies or for a group of public authorities, taking into account their structure and size.

Any organisation is able to appoint a DPO. Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to discharge your obligations under the GDPR.

What are the tasks of the DPO?

The DPO's minimum tasks are defined in Article 39:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

What does the GDPR say about employer duties?

You must ensure that:

- 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 task.

- Adequate resources are provided to enable DPOs to meet their GDPR obligations.

Can we allocate the role of DPO to 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 also contract out the role of DPO externally.

Does the data protection officer need specific qualifications?

The GDPR does not specify the precise credentials a data protection officer is expected to have.

It does require that they should have professional experience and knowledge of data protection law. This should be proportionate to the type of processing your organisation carries out, taking into consideration the level of protection the personal data requires.

Further Reading

Relevant provisions in the GDPR - see Articles 37-39 and 83 and Recital 97
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 on DPOs and FAQs on DPOs.

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.

Security

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

The ICO has previously produced guidance to assist organisations in securing the personal data they hold. We are working to update existing guidance to reflect GDPR provisions and once completed, this section will expand to include this information.

In the meantime, the existing guidance is a good starting point for organisations. This is located in the guidance index under the 'security' heading.

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 and this unavailability has a significant negative effect on individuals.

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.

The Article 29 Working Party has published guidelines on personal data breach notification. The consultation period has now closed. 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.

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?

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.