Data Protection and PECR Training
Supporting notes and further reading
Module 3 : lawful processing

Introduction

These notes are designed to set out the key points covered during module 3 of our data protection online training programme. These notes are not designed to replace the online module, but are intended to be a point of reference for your follow-up study. You may find it helpful to have these notes and the relevant legislation open whilst watching the online module:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018 (DPA)

This document contains:

Supporting notes

Module 3 looks at principle (a) and lawful processing. It covers:

Article 5(1) principle (a)

Article 5(1) principle (a) states that in relation to the data subject, personal data shall be processed:

- lawfully;
- fairly; and
- in a transparent manner.

This is an important principle because it specifically concerns the processing of data. We get a lot of complaints about processing that is considered not to be fair or lawful.

A complainant will often argue that they had no idea the processing was taking place or that the processing was not something they would reasonably expect.

We will look at each of these elements in turn but they do overlap. For example, if processing is not transparent, it is unlikely to be fair and will not be lawful.

Fair and transparent

The two concepts of fairness and transparency are inextricably linked - transparency leads to fairness.

Transparent processing is about being clear and honest with individuals about how their information will be used. The UK GDPR lists what information a controller must give a data subject when personal data is collected - for example, if the data will be shared and what their rights are.

The controller must consider how it will provide this privacy information to the data subject. It is usually provided in a Privacy or Transparency Notice.

But fairness is more than just transparency – it also means the personal data must be processed in a fair way. A controller must consider how the processing affects the interests of the people concerned both as a group and individually. It should ask itself what processing the data subject should reasonably expect.

The controller must also consider whether the processing will have an unjustified adverse effect upon an individual.

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

For example, where personal data is collected to assess tax liability, to impose a fine for breaking the speed limit, or for debt-collecting activities, the information is used in a way that may cause detriment to the individuals concerned. However, the proper use of personal data for these purposes will not be unfair, as people should reasonably expect processing for these sorts of purposes.

Unlawful processing in terms of other legislation

If processing involves committing a criminal offence, it will obviously be unlawful.

Other examples of where processing may be unlawful are where it results in:

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

The ICO does not generally take action for infringements of other legislation. Many areas of law are complex, and fall outside of the ICO's remit.

But lawfulness is key to compliance and so any breaches of other laws does also mean a failure to comply with principle (a).

Lawful processing in terms of Article 6

In order for processing to be lawful, a controller must be able to identify at least one of the Article 6 lawful bases for processing.

These are:

(a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;

Or processing is necessary for:

(b) the performance of a **contract** that the data subject is party to;

(c) compliance with a **legal obligation;**

(d) the protection of the **vital interests** of individuals (where the processing is a matter of life and death);

(e) the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This is known as **public task**. An example is the council processing your council tax details;

(f) **legitimate interests**. This states that processing is necessary for the purposes of the legitimate interests pursued by the controller or

by a third party. These interests must be weighed against the interests or fundamental rights and freedoms of the data subject so this basis involves some judgement and a balancing test called a legitimate interests assessment or LIA.

Lawful bases (b) to (f) depend on the processing being "necessary" for that particular purpose. This means the processing must be a targeted and proportionate way of achieving the purpose.

General points about choosing a lawful basis

- No basis is more important than others – the controller must pick the one which is most appropriate for the circumstances.
- A controller must determine its lawful basis before it begins processing, and should document it.
- It is up to the controller to decide which lawful basis applies. This will depend on the controller's specific purposes and relationship with the individual. It might consider that more than one basis applies, in which case it should identify and document all of them from the start.
- The controller should take care to get it right first time – it should not swap to a different lawful basis at a later date without good reason. In particular, a controller cannot usually swap from consent to a different basis.
- A controller should ensure that its privacy information includes the lawful basis for processing as well as the purposes of the processing.

For example, a university may consider a variety of lawful bases for its processing, depending on what it wants to do with the data it holds. It 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.

Consent

The definition of consent contains a number of key phrases:

- consent must be freely given, specific, and informed;
- it must be an unambiguous indication of the data subject's wishes; and

- agreement to the processing must be given in a statement or clear affirmative action.

Freely given

If the individual has no real choice about the processing, consent is not freely given and will be invalid.

This means a person must be able to refuse consent without detriment.

It also means controllers in a position of power over individuals should avoid relying on consent unless confident they can demonstrate it is freely given.

For example, the ICO will never ask you for consent to monitoring at work. This is because, as an employer, it has a position of power over you and you may not feel you can refuse. In this situation, consent would not be freely given.

In another example, the ICO might ask you if you would like to take part in a recruitment video for our website. It makes it clear that there is no requirement for any staff to take part in it, and participation would not be taken into account for performance review purposes. As participation is optional, and there are no adverse consequences to those who do not want to take part, the ICO could consider consent.

Specific and informed

The individual should be informed of:

- the controller's identity
- the purposes of the processing
- the processing activities

They should be told exactly what processing they are consenting to. Separate consent will be needed for different processing operations wherever appropriate. Where possible, a controller should provide granular consent options for each separate type of processing, unless those activities are clearly interdependent.

The controller must clearly explain to people what they are consenting to in a way they can easily understand. The request for consent needs to be prominent, concise, separate from other terms and conditions, and in plain language.

Unambiguous indication (by a statement or clear affirmative action)

It must be obvious that the individual has consented to the processing and this requires more than just a confirmation that they have read the terms and conditions.

For consent to be valid it must be both unambiguous and affirmative. It must be clear that the individual deliberately and actively chose to consent.

There must be a clear signal that they agree and if there is any room for doubt, it is not valid consent.

A clear affirmative action can include:

- signing a consent statement;
- oral confirmation;
- ticking a box when visiting an internet website;
- a binary choice presented with equal prominence, or
- switching technical settings away from the default.

The key point is that all consent must be opt-in consent – failure to opt out is not consent and so pre-ticked boxes to indicate consent are banned under the UK GDPR.

For example, you order something online and there is a pre-ticked box which says 'I consent to receive special offers'. This means you will receive the offers by default unless you actively untick the box. This is not allowed – the controller cannot use pre-ticked boxes relying on silence, inactivity or default settings and then claim the processing is based on consent.

Further consent requirements

- A controller must be able to demonstrate that the data subject has consented to the processing.
- It will need to keep a record of consent which means a record of who consented, when, how it was given, and what the individuals were told at the time.
- The data subject has the right to withdraw their consent at any time and the controller must make them aware of this.

- It must be as easy to withdraw consent as it is to give it.

Children's consent when accessing an 'information society service' or ISS

Article 8 refers to children's consent when they are accessing an 'information society service' or ISS. An ISS is defined in full in our guidance, but basically it is an online service provided at a user's request – for example a social media account or an internet game site.

In the UK, where an ISS is offered directly to a child aged between 13 and 17, they can give their own consent to the processing of their personal data.

If a child is under 13, the controller must get consent for processing from someone with parental authority for that child. It is not lawful for the child to give their own consent.

This does not apply in the context of preventive or counselling services offered directly to a child.

In cases where a controller wishes to rely on consent for processing, Article 8 states that it will need to make 'reasonable efforts' to verify parental responsibility for those under the relevant age.

This means a controller may need to implement age-verification measures.

This only applies where the controller chooses to use consent as the lawful basis – so for example, the controller might use legitimate interests for all its processing, irrespective of the child's age.

The ICO has produced an Age Appropriate Design Code or Children's Code to ensure that online services likely to be accessed by children are appropriate for their use and meet their development needs.

Children and other types of (non-online) processing

For other types of (non-online) processing, the general rule in the UK is that organisations should consider whether the individual child has the competence to understand and consent to processing for themselves.

We take the view that a child aged 12 and over is likely to have the required level of understanding to provide their own consent to processing.

This is not an absolute rule, but we consider it to be a reasonable approach. It reflects the law in Scotland where children aged 12 or over are presumed to be of sufficient age and maturity to exercise their data protection rights (unless the contrary is shown).

This is discussed in more detail in the module which covers the right of access.

Four problematic consent statements

1. **Untick the box if you don't want to receive any marketing material from us.**

   - Remember consent should be given by a clear affirmative act and pre-ticked boxes do not constitute valid consent.

2. **We'd like to pass your details on to our carefully selected third parties. Please tick here to agree.**

   - This raises the question - why are details being passed to third parties? Consent needs to be specific and informed and so controllers must identify themselves and also identify any third parties, explaining why data will be shared. For consent to be valid, it would also have to be given separately for each named third party organisation.

3. **Once you have given us permission to use your data in this way, you cannot change your mind.**

   - This is incorrect because the data subject does have the right to withdraw their consent at any time. If the controller can't action withdrawal of consent then it cannot use consent.

4. **To process your loan we need your consent to contact credit reference agencies.**

   - So with this example, if a customer refuses or withdraws their consent, the credit card company will still want to send the data to the credit reference agencies on the basis of its 'legitimate interests'. So asking for consent is misleading and inappropriate – there is no real choice. The company should have relied on 'legitimate interests' from the start. To ensure fairness and transparency, the company must still tell customers this will happen, but this is very different from giving them a choice in data protection terms.

Contract

Lawful basis (b) states that 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.

Examples include:

- a bank processing your details;
- a shop processing your details to fulfil an order for goods bought;
- your employer processing your details in order to pay you; and
- a car insurance broker providing a quote. It will need to process certain data in order to prepare the quotation – such as the make and age of the car and your driving background and this means it is processing at the request of the data subject prior to entering a contract.

The processing must be necessary for the performance of the contract. For example, if you buy something online, the organisation will process your address and credit card details in order to take payment and deliver the goods. This processing is necessary in order to perform the contract. However, the profiling of your interests and preferences based on items purchased is not necessary for the performance of the contract and the organisation cannot rely on this basis for such processing. It might instead ask for your consent.

Legal obligation

The next basis for processing is (c) - compliance with a legal obligation.

This is where an organisation can process data for a particular purpose if they are required by UK law.

There are a few important points to consider:

- It is likely to be clear from the law in question that the processing is actually necessary for compliance.
- If the law is optional and not obligatory, then a controller cannot rely on legal obligation.

- When processing on this basis, the individual has no right, for example, to erasure or to object to the processing. This is because the legal requirement means controllers must process and keep the data.

- It's important to understand that the rights individuals have will change, depending on the lawful basis.

Examples include:

- an employer must comply with its legal obligation to disclose employee salary details to bodies such as HMRC;
- a financial institution is obliged to report money laundering;
- a company has a legal obligation to monitor equality of opportunity in the organisation; and
- an organisation has a legal obligation to comply with a court order.

Vital interests

The lawful basis (d) is vital interests.

This allows organisations to process personal data if it is necessary to protect someone's life. This could be the life of the data subject or someone else.

Examples include:

- the recording of treatment of an unconscious traffic accident victim in A&E;
- processing for humanitarian emergencies - for monitoring epidemics and their spread;
- or in situations such as during a natural or man-made disaster; and
- the disclosure of medical information in a medical emergency.

Public task

If organisations need to process personal data to carry out their official functions or a task in the public interest – and they have a legal basis for the processing under UK law – then they can use this basis.

For UK public authorities, our view is that the public task basis is likely to apply to many if not all of their activities.

However it does relate to the function, not the type of organisation – for example a private water company has a task which it performs in the public interest.

Examples include:

- a council processing council tax data;
- the DWP recording a claim for universal credit;
- a school processing children's exam results; and
- the ICO processing complaints.

If relying on public task, the controller must be able to point to the underlying UK legal provision.

A public authority cannot rely on legitimate interests in circumstances where public task applies.

Also a controller can't point to someone else's 'public task or function' and use that to justify its reliance on this basis.

Legitimate interests

The final bases for processing is (f) - legitimate interests. This is the most flexible lawful basis, but a controller cannot assume it will automatically cover all of its processing.

A wide range of interests may be legitimate interests. They can be the controller's own interests or the interests of third parties. They can be commercial interests as well as the wider interests of society.

However the use of this basis involves the balancing of the controller's legitimate interests against the interests and rights or freedoms of the data subject.

So it involves a balancing test.

Examples include:

- a debt collection agency track down an individual with debts;
- an employer processing emergency contacts;
- a shop passing CCTV footage of a crime to the Police; and
- a lender such as a credit card company sending personal data to credit reference agencies.

The legitimate interests assessment

The balancing test is a three-part test and is known as a legitimate interests assessment or LIA. It is a type of risk assessment based on the specific context and circumstances of the processing.

Our guidance gives examples of the types of questions a controller should ask themselves for each part of the test.

With respect to the purpose test, the controller might ask:

- Why does it want to process the data – what is it trying to achieve?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing? and
- How important are those benefits?

The next part of the test is the necessity test and here the controller must ask:

- Whether the processing actually helps meet the identified interest; and
- Whether the processing is a reasonable way to go about it?

Finally the balancing test involves asking:

- What is the nature of the personal data? Is it particularly sensitive or private?
- What are the reasonable expectations of the individual?
- What is the possible impact of the processing on the individual?
- Can any safeguards can be put in place to mitigate any negative impacts?

The LIA and the questions a controller must ask are discussed in the guidance. Once the controller has considered the questions, it must decide if the interests it has identified are overridden by the rights and freedoms of the data subject.

For example, if a company is investigating a complaint about one of its employees, it has a legitimate interest to process the personal data of the individual concerned. In these circumstances, the rights and freedoms of the individual do not override the need for the company to consider the complaint. An employee should have a reasonable expectation that the company would investigate and clear their name or take steps to address the issue.

Back to top

Further reading

In the Guide to the UK GDPR have a look at the section 'lawfulness, fairness and transparency'. Read the 'In brief' questions and answers.

Now go back to page Guide to the UK GDPR and this time click on the link 'Lawful basis for processing'. Read the 'At a glance' and 'Checklists'.

Find an example in the guidance of a company who wants to change its lawful basis from consent to legitimate interests (see the yellow boxes for examples).

Note in the 'At a glance' section, there is a link to our lawful basis interactive guidance tool'. Have a look at this.

Read the section 'Why is the lawful basis for processing important?' and note how the lawful basis chosen can affect the rights of the data subject.

Read the section 'Can we change our lawful basis?' and 'What happens if we have a new purpose?' We are often asked these questions.

Now look at each of the bases on the left. There is a lot of guidance on consent. Look at the 'in detail' section for consent and read some of these paragraphs.

Find two examples in the guidance where an unambiguous indication of consent is given by a clear affirmative action (see the yellow boxes for examples).

Find an example in the guidance where consent is inappropriate as a basis for processing because it has been made a condition of service.

Read the in brief paragraphs for contract, legal obligation, vital interests and public task.

There is also detailed guidance on legitimate interest. Have a look at some of these questions and answers.

In particular look at the question 'Can public authorities use legitimate interests?'

Find an example in the guidance where a charity decides to use legitimate interests for its marketing purposes (see the yellow boxes for examples).

For more information on the LIA, follow the link on the left 'How do we apply legitimate interests in practice?' There are some useful examples in this section.

Optional further reading

For more information about the processing of children's personal data, please see the section on 'Children' and the 'Age Appropriate Design Code' in the section 'Key data protection themes'.

Also see our self-paced training on the Age Appropriate Design Code which is available via i-Learn.

Back to top

KNOWLEDGE SERVICES
UPDATED: 29 APRIL 2022