Legal basis for processing

In brief

What is your legal basis for processing?

The legal bases for processing personal data are set out in schedule 2 of the DPA. Principally, all of the conditions are equal so that none is preferable to any other. At least one of these conditions must apply whenever you process personal data:

- Consent: the individual has given clear consent for you to process their personal data for a specific purpose;
- Contract: the processing is necessary for performance of a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract;
- Legal obligation: the processing is necessary for you to comply with a law (not including contractual obligations);
- Vital interests: the processing is necessary to protect the individual’s life;
- Public functions: the processing is necessary for you to perform a public function, or a function of a public nature exercised in the public interest;
- Legitimate interests: Processing necessary for legitimate interests pursued by the data controller or a third party, except where it is unwarranted because of prejudicing the rights and freedoms or legitimate interests of the individual.

The legal bases for processing sensitive personal data are set out in schedule 3 of the DPA. At least one of these conditions, in addition to a condition for processing above, must apply whenever you process sensitive personal data:

- Consent: the individual has given clear consent for you to process their sensitive personal data for a specific purpose;
- Employment: the processing of sensitive personal data imposed by law in the context of the individual’s employment;
- Vital interests: the processing of sensitive personal data is necessary to protect the vital interests of the individual or any other person where consent cannot be given, cannot reasonably be obtained, or has unreasonably been withheld;

- Non-profit organisations: the processing of sensitive personal data is carried out by certain types of non-profit organisation and relates to individuals who are their members or individuals who are in regular contact with the organisation. This does not cover disclosure to a third party without consent from the individuals concerned;
- Made public: processing of sensitive personal data that has been made public by the individual;
- Legal proceedings: processing of sensitive personal data is necessary for legal proceedings, legal advice or legal rights;
- Public functions: processing of sensitive personal data is necessary for public functions;
- Medical: processing of sensitive personal data by a health professional or someone who owes an equivalent duty of confidentiality is necessary for medical purposes.

When is processing "necessary"?

Many of the legal bases for processing depend on the processing being "necessary". This means that the processing must be a targeted and proportionate way of achieving the purpose. The legal 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.

Example

An application for a credit card requires you to provide the name and contact information of your closest living relative. This information is not necessary for the decision whether to grant or to reject your application.

How do you decide which legal condition applies?

Which legal condition applies will depend on the circumstances and the context of the processing, including these factors:

What is your purpose of processing – what are you trying to achieve by processing the personal data?

- 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?
- What type of organisation are you?

There is not one-size-fits-all, and there may be more than one applicable legal condition for processing. No one legal condition for processing is better, safer or more important than another, and there is no hierarchy in

the listing of the conditions, except to an extent regarding processing necessary for the exercise of public functions.

Several of the legal 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 Cayman Islands Act, then you are able to use the "public function" 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 prohibition on public authorities using consent or legitimate interests as their lawful basis.

For the purposes of the DPA, the term "public authority" has the same meaning as the definition in the *Freedom of Information Act (2021 Revision).*

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.

The University may be a public authority, so the "public functions" legal 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 functions" 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 legal basis for processing 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 functions, 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 the individuals vulnerable?
- Are some of the individuals concerned likely to object?
- Are you able to stop the processing at any time on request?
- To what extent is the processing unavoidable or mandatory?

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. You should avoid relying on consent when the individuals are unable to give a proper consent (see below on conditions for consent), or the individuals have no genuine choice in the matter.

When should you decide your legal basis for processing?

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

Example

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

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

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

this is the case then you should be aware of it.

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 (to the extent it is practicable to do so) and document the change.

What happens if you have a new purpose for processing personal data?

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, if you rely on consent, you must make sure that the consent is freely given, specific, informed, and unambiguous. Thus, if you want to repurpose personal data which you previously obtained by relying 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 with the original purpose.

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

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

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 a new legal basis to process the data for that new purpose.

The DPA specifically says that further processing for the following purposes is considered compatible lawful processing:

- Research purposes ('research' is understood to be scientific research);
- history (archiving) purposes;
- statistical purposes.

There is a link here to the 'purpose limitation' principle in the second data protection principle which states that "Personal data shall be obtained only for one or more specified lawful purposes, and shall not be further

processed in any manner incompatible with that purpose or those purposes."

How should you document the legal basis of your processing?

Under the DPA you are not required to document upfront that you are in compliance with the Act, or have appropriate policies and processes. However, clear, upfront documentation of all aspects of your personal data processing activities will be very helpful when one of the individuals whose data you process exercises their rights under the Act, when a data breach occurs, or when you are subject of an investigation by the Ombudsman.

Therefore, it is best practice to document the legal basis of all your personal data processing, for each purpose, upfront. 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. A good practice would be to include the legal basis in the privacy notice you make available to the data subjects. 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.

Relevant provisions

Data Protection Act (2021 Revision)

Schedule 2: Legal conditions for processing personal data

Schedule 3: Legal conditions for processing sensitive personal data

Further Guidance

ICO: Lawful basis interactive guidance tool