ABU DHABI GLOBAL MARKET

LAWFUL BASIS FOR PROCESSING PERSONAL DATA AND SPECIAL CATEGORIES OF PERSONAL DATA

What is a Lawful Basis for Processing?

The ADGM Data Protection Regulations 2021 requires all ADGM Establishments processing personal data to rely upon a valid lawful basis for each of their processing activities. A lawful basis is a legitimate reasons or conditions under which data may be processed. Processing without reliance on a basis is not permitted.

There are six lawful bases for processing which are set out in section 5(1) of the DPR 2021. Data Subjects have to be informed of the lawful basis you are using as part of their right to be informed. If you are processing special category personal data, you also need to identify an additional condition which applies to the processing from the list set out in section 7(2) of the DPR 2021.

What are the various Lawful Bases for Processing?

CONSENT

This legal basis applies where the Data Subject has given consent to the processing of their personal data for one or more specific purposes. The Regulations set specific conditions for consent and if you do not meet these conditions, any consent obtained will be invalid.

Consent must be:

1. Freely given – this means that the Data Subject must have a genuine, free choice about whether they want to consent to the processing. This may not be the case if:

Refusing consent leads the individual to suffer a detriment

The performance of a contract is conditional on the Data Subject consenting, in circumstances where the processing is not necessary for the performance of that contract; or

There is an imbalance of power in the relationship between the Controller and Data Subject such that the Data Subject may not feel they can refuse (e.g., as may be the case in the relationship between an employer and employee or a public authority and citizen).

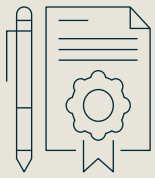
Example:

An organisation asks its employees for consent to share their bank details with an outsourced payroll provider which the organisation uses to make salary payments to its employees.

Consent in this context cannot be considered freely given due to the imbalance of power in the relationship between the employer and its employees and also because the employees risk not being paid if they refuse.

In this case, consent is not the appropriate legal basis for the processing. The organisation should instead consider the “legitimate interests” legal basis.

2. Specific: Specific consent means consent which relates to a particular processing activity/activities. The Data Subject needs to understand the purposes for which Controller intend to process their data before they are asked for or give consent. If Controller is asking for consent to more than one processing activity, it may be appropriate to offer a granular choice, meaning that the individual can choose whether or not to consent on a per-activity basis.



Example:

A business which sells goods via its website posts a privacy policy on its website which explains all the different purposes for which it processes customers' personal data. When a person signs up for an account on the website, they are asked to tick a box to indicate they consent to the business processing personal data "as described in the privacy policy". This consent will not be valid as it is not specific.

3. Informed: This means telling Data Subjects about the processing before you ask for their consent. As a minimum you should tell individuals the identity of the Controller(s) that will rely on the consent, the purposes for which the personal data will be processed and that they can withdraw their consent at any time.

Example:

A business wants to be able to send marketing emails to customers. When customers buy a product and provide their contact details on an electronic form, there is a statement that the business considers that they have consented to the sending of marketing emails unless the individual sends an email or rings a number to object.

This will not be valid consent. There is no statement or clear affirmative action from the Data Subject. Additionally, this purported method of gaining consent relies on inaction by the Data Subject (i.e., the individual not objecting). This is not permitted.

Consent can be given in writing, electronically (e.g., by submitting a form, ticking a box etc.) or orally. What is important is that there is some action required by the Data Subject and the Data Subject understands that by doing the action, they are indicating consent. Silence, inaction and pre-ticked boxes do not constitute consent.

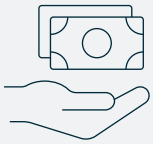
Data Subjects have the right to withdraw their consent at any time, and it must be as easy to withdraw consent as it was to give it in the first place. You must ensure you tell people how they can withdraw their consent. You need to keep records of consent and withdrawals of consent so that you can demonstrate that Data Subjects have consented to your processing.

PERFORMANCE OF CONTRACT

This legal basis applies where processing is necessary:

- for the performance of a contract to which the Data Subject is a party, or
- in order to take steps at the request of the Data Subject prior to entering into a contract

This legal basis is likely to apply where you process personal data so that you can comply with your obligations under a contract with the Data Subject, or you process personal data to enable a Data Subject to comply with their obligations under a contract with you (e.g., you process payment details so that the individual can pay you).



Example:

An online retailer sells products via its website. When a customer buys a product the retailer processes the customer's personal data such as name, payment card details, billing and shipping address etc. so it can fulfil the customer's order.

This processing is necessary to perform the contract for the sale of goods with the customer.

It also applies where you do not yet have a contract with the individual, but the individual has asked you to do something because they are considering entering into a contact with you (even if they don't enter the contract in the end).

LEGAL OBLIGATION

This legal basis applies if the processing is necessary for compliance with a legal obligation to which the Controller is subject under applicable law:

- in ADGM, or
- under Abu Dhabi or UAE Federal Law having application in ADGM.

as such enactment/subordinate legislation applies to Controllers and Processors which are subject to the DPR 2021.

This legal basis applies where you are required to process personal data in order to comply with a law which falls within the above definition. You should be able to identify the legal obligation in question if you intend to rely on this basis.

VITAL INTERESTS

This legal basis applies where the processing is necessary to protect the vital interests of the Data Subject or of another natural person.

Although not defined in the DPR 2021, vital interests are intended to cover interests which are essential to someone's life, i.e., a matter of life or death. It is likely to be particularly relevant in the context of the provision of emergency medical care. In contrast, for pre-planned medical care, consent is likely to be the appropriate legal basis.

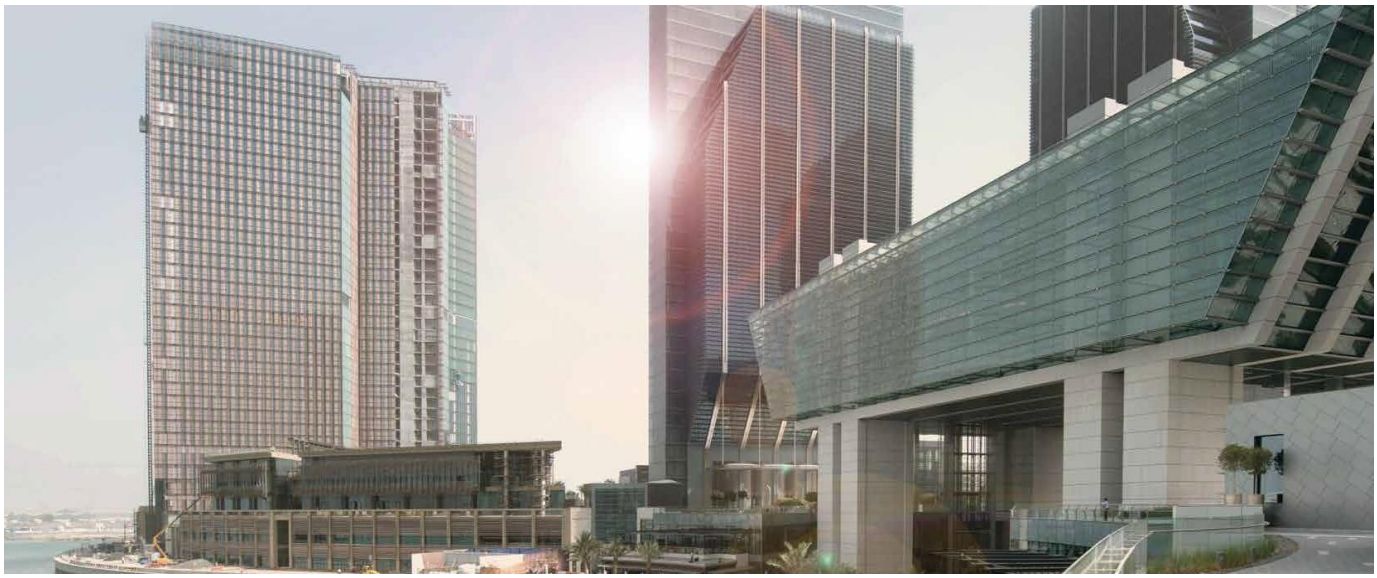
You should be aware that where you are processing personal data relating to health, you also need to find an additional condition for the processing of special category personal data from section 7 of the DPR 2021.

PUBLIC TASK

This legal basis applies where processing is necessary:

- for the performance of a task carried out by a public authority in the interests of ADGM
- in the exercise of ADGM's functions
- in the exercise of the Financial Services Regulatory Authority's functions
- in the exercise of the ADGM Court's functions
- in the exercise of the Registration Authority's functions, or
- in the exercise of official authority vested in the Controller under applicable law

This legal basis will mainly apply to public authorities, and the bodies listed in the bullet point list above. In some cases it may also apply to private sector organisations but only where they are acting under official authority.



LEGITIMATE INTERESTS

This legal basis applies where the processing is necessary for the purposes of legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or rights of the Data Subject which require protection of personal data, in particular where the Data Subject is a child.

If you want to rely on the legitimate interest basis you need to identify your legitimate interest and balance these against the interests of the Data Subjects. This can be done by carrying out the three-part test explained below. You can only rely on the legitimate interest basis where you have satisfied the above three-part test. It is recommended that you document this consideration in writing. This is referred to as a legitimate interest assessment or LIA.

Purpose test

Identify the relevant legitimate interest that you are pursuing:

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

Necessity test

Consider whether your processing is necessary to achieve the purpose/interest:

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

Balancing test

Consider whether the Data Subject's interests override your legitimate interest:

- 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 and how big is the impact?
- Are any of the individuals children or vulnerable in any other way?
- Can you adopt any safeguards to minimise the impact?
- Can you offer an opt-out?

Special Categories of Personal Data

The DPR 2021 defines the following as special categories of personal data:

- personal data revealing **racial or ethnic origin**
- personal data revealing **political opinions**
- personal data revealing **religious or philosophical beliefs**
- **genetic data**
- **biometric data** (where used for identification purposes)
- data concerning **health**
- data concerning a person's **sex life** or **sexual orientation**
- personal data relating to **criminal convictions and offences or related security measures**

If you want to process special category personal data, as well as finding a relevant lawful basis from the Regulations, you also need to be able to find a relevant condition from section 7(2) of the DPR 2021 which are explained in more detail below.

Remember also that you must do a data protection impact assessment (DPIA) for any type of processing that is likely to be high risk. You are more likely to need a DPIA for processing of special category data. For further information please see Part 4 of the Guidance (Data Protection Impact Assessments).

Lawful Bases To Process Special Categories of Personal Data

EXPLICIT CONSENT

You can process special categories of personal data if the Data Subject has given explicit consent to the processing for the specified purposes.

- Explicit consent must be confirmed in words rather than inferred from an action
- The consent statement must specify the element of the processing which requires consent e.g., the nature of the special category personal data.
- If you obtain explicit consent orally you must keep a record of the wording used

Example:

A make up retailer asks customers about skin conditions so that it can recommend appropriate products to them. On the form that customers fill out, the retailer uses the following consent statement:

Please tell us about any skin conditions you have so that we can take these into account when recommending the best products for you.

……

☐ *I consent to you using the above information to recommend products.*

EMPLOYMENT LAW

You can process special categories of personal data where 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 law, provided that when the processing is carried out, the Controller has an appropriate policy document in place. If you rely on this condition you must be able to identify the relevant law which requires or permits the processing.

Example:

An employer processes data which reveals a person's race/ethnicity as part of its checks to confirm that employees have the right to work in ADGM. It is required to carry out these checks by law.

VITAL INTERESTS

You can process special category personal data where necessary to protect vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.

HEALTH PURPOSES

You can process special categories of personal data where necessary for health purposes, including the below. To rely on this condition, the processing must be carried out by or under the responsibility of a health professional subject to the obligation of professional secrecy or duty of confidentiality.

- preventative or occupational medicine
- the assessment of the working capacity of an employee
- medical diagnosis
- the provision of health care or treatment
- the management of healthcare systems or services
- pursuant to a contract with a health professional

Example:

A business arranges for an employee who is recovering from an accident to have an assessment by an occupational therapist prior to the employee's return to work, to determine if the employee is fit to return to work and whether the business needs to make any changes to the working environment.

The occupational therapist can rely on this condition to process the employee's health data as the occupational therapist is a health professional and is subject to professional secrecy obligations.

PUBLIC INTEREST IN THE AREA OF PUBLIC HEALTH

You can rely on this condition where the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.

If you rely on this condition you must be able to demonstrate that there is a public interest in the area of public health in the processing you are carrying out. The term "public interest" is not defined but you need to be able to show a benefit to wider society/the public as a whole.

"Public health" is likely to cover things such as health status including morbidity and disability, the elements which affect health status, healthcare needs, resources allocated to healthcare, the provision of and universal access to healthcare, healthcare expenditure/financing, and the causes of mortality.

Example:

A manufacturer of medical devices maintains records of reports of problems or malfunctions of devices which are being used in healthcare settings. The reports it receives contain personal data of the patients using the devices, including data relating to health. This processing is necessary for reasons of public interest in the area of public health to ensure high standards of medical devices.

ARCHIVING AND RESEARCH PURPOSES

You can rely on this condition where the processing is necessary for Archiving and Research Purposes in accordance with applicable law, The phrase "Archiving and Research Purposes" means:

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

NOT-FOR-PROFIT BODIES

You can rely on this condition where the 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 including religious, cultural, educational, social or fraternal purposes or for other charitable purposes 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
- the personal data is not disclosed outside that body without the consent of the Data Subjects.

This condition is not purpose based like most of the others. Rather it applies to certain processing carried out by not-for-profit organisations. Because it is not purpose based, there is no necessity test.

The phrase "legitimate activities" is not defined in the DPR 2021, however, the processing must be within the confines of the purposes and powers of the organization as set out in its constitution or other similar document, and must not be unlawful or unethical in any way.

DATA THAT HAS INTENTIONALLY BEEN MADE PUBLIC

You can rely on this condition where you are processing personal data which is intentionally made public by the Data Subject.

This condition does not allow you to process all special category personal data in the public domain but only that which the Data Subject him/herself has made public. Note that the individual must also have made the data public intentionally for you to be able to rely on this condition. If you rely on this condition, you should keep a record of where and how you obtained the data you process.

PERFORMANCE OF A CONTRACT

You can process special categories of personal data where processing is necessary:

- for the performance of a contract to which the Data Subject is party
- in order to take steps at the request of the Data Subject prior to entering into a contract.

Example:

A person requests a quote from an insurance provider for private healthcare insurance. The insurance provider needs to process details about the person's medical conditions in order to assess whether and on what basis it can offer cover. The insurance company can rely on the "performance of a contract" condition as it is processing the data on the request of the individual prior to entering a contract with them.

This legal basis is likely to apply where you process personal data so that you can comply with your obligations under a contract with the Data Subject, or you process personal data to enable a Data Subject to comply with their obligations under a contract with you.

The performance of a contract legal basis only applies where you are processing the personal data of the person with whom you have or may in future have a contract. It cannot be relied upon if you need to process one person's data but your contract is with another person. Nor can it be relied upon where you take steps at your own initiative, rather than at an individual's request, prior to entering into a contract with that individual.

COURTS AND LEGAL CLAIMS

You can rely on this condition where the processing is necessary for the establishment, exercise or defense of legal claims or whenever the courts are acting in their judicial capacity.

Example:

A lawyer is representing a client who is accused of fraud. The lawyer relies on this condition to process details of the client's previous criminal convictions when preparing for the hearing relating to the current alleged offence.

SUBSTANTIAL PUBLIC INTEREST

To rely on this condition (unless specified otherwise) the Controller must have in place an "appropriate policy document" as per section 7(3) of the DPR 2021 when the processing is carried out.

You can rely on this condition where the processing is necessary for one of the reasons of substantial public interest set out in the list contained in section 7(2)(k) of the DPR 2021. You do not need to carry out your own assessment of, or be able to demonstrate that the processing is in, the substantial public interest, provided that one of the specific purposes applies.

Many of the specific reasons in section 7(2)(K) of the DPR 2021 only apply where the Controller cannot get the Data Subject's consent for some reason. Examples of why this might be the case include because it would tip off a person who is under investigation, prejudice an investigation, or that it might not be possible to get valid consent in the circumstances e.g., because the Data Subject is an employee of the Controller and the imbalance of power in the relationship means that the consent may not be freely given.

Note: Appropriate Policy Document

Certain of the conditions for processing special category personal data require the Controller to have an appropriate policy document in place if the Controller wants to rely on that condition. An appropriate policy document is a short document which sets out your approach to the processing of the special category data which is based on the condition which requires the document.

There are no particular requirements as to the form of the document, but it must explain:

- which of the conditions you are relying upon
- how you comply with the principles in section 4 of the DPR 2021 (the data processing principles)
- your policies relating to retention and erasure of personal data. You can find out more about retention in the Guidance published by the ODP

You must have the appropriate policy document in place at the time you start processing the personal data and retain it for at least 6 months after you stop such processing. During this time you must review and update it as appropriate and make it available to the Commissioner of Data Protection if requested.

If you process special category personal data for various purposes you do not need a separate policy document for each, you can prepare one document which covers all processing activities.

The Commissioner has developed a standalone appropriate policy document guide and template for you to use. For more information about the appropriate policy document requirement and a copy of the template is available on the Guidance Page of the Office of Data Protection website.