ABU DHABI GLOBAL MARKET

Guidance on the Data Protection Regulations 2021

Part 1:

- Overview of the Data Protection Regulations 2021 and Guidance
- Key terms and concepts
- Scope
- Principles of processing
- Lawful bases for processing/special categories of personal data

Office of Data Protection

TABLE OF CONTENTS

1. OVERVIEW OF THE DPR 2021 AND GUIDANCE

Introduction to this guidance

1.1 This is Part 1 in the series of guidance (Guidance) on the Abu Dhabi Global Market Data Protection Regulations 2021 (DPR 2021).

Introduction to Abu Dhabi Global Market

1.2 Abu Dhabi Global Market (ADGM) is a broad based international financial centre, established pursuant to Abu Dhabi Law No. 4 of 2013 in the Emirate of Abu Dhabi. With its own civil and commercial laws based on the English common law, ADGM offers the local, regional and international business community a world-class legal system and regulatory regime.

About this Guidance

1.3 Who the Guidance is aimed at

This Guidance is for anyone within an ADGM-established entity which collects and processes personal data who has day to day responsibility for personal data. It is aimed at small and medium enterprises although it may also be useful for larger organisations and their legal advisors.

In some cases, businesses outside the ADGM may also have to comply with the DPR 2021, so this Guidance may also be useful for those organisations. You can find more details of when the DPR 2021 applies to businesses outside the ADGM in paragraph 3 (Scope) of this document.

1.4 What the Guidance does

This Guidance aims to explain how the DPR 2021 work and help you understand how your organisation can comply with them. It will not tell you exactly what to do because the DPR 2021 recognise that every organisation is different, and therefore allow for some flexibility.

This flexibility means that you need to think about, and take responsibility for, the specific ways you use personal data. Whether and how you comply depends on exactly why and how you use the data. There is often more than one way to comply with the DPR 2021.

This Guidance includes examples to help you ask the right questions, and understand your options, but it is up to each organisation to decide what they will do and be able to justify these decisions. This is a key principle of data protection law, known as the accountability principle.

In addition to your organisation's obligations under the DPR 2021, you should consider your obligations under data protection regulations outside the ADGM. The Commissioner of Data Protection recommends organisations obtain independent legal advice to fully understand their data protection obligations both inside and outside the ADGM.

1.5 How the Guidance is set out/structured

The Guidance is contained in a number of separate documents, each of which covers a different topic or group of topics.

The suite of Guidance broadly follows the order that topics appear in the DPR 2021 and includes examples to help explain how the DPR 2021 applies and help you make sure you consider all relevant aspects. It is made up of the following documents:

Part 1

- Overview of the DPR 2021 and Guidance (see paragraph 1 of this document)
- Key terms and concepts (see paragraph 2 of this document)
- Scope (see paragraph 3 of this document)
- Principles of processing (see paragraph 4 of this document)
- Lawful bases for processing/Special categories of personal data (see paragraph 5 of this document)

Part 2

- Data subjects' rights

Part 3

- Data protection by design and by default
- Data protection fee
- Record of processing activities
- Data protection officers
- Processors

Part 4

- Data protection impact assessments

Part 5

- Security of processing
- Cessation of processing
- Personal data breach notifications

Part 6

- International transfers of personal data

Part 7

- Codes of conduct and certification
- Role of Office/Commissioner of Data Protection

Part 8

- Individuals' rights and remedies

1.6 Alignment of DPR 2021 with GDPR

When preparing the DPR 2021, the ADGM carried out an international benchmarking study of international standards and best practice and concluded that the EU's GDPR is the leading international standard and represents best practice for robust data protection legislation. The DPR 2021 are closely based on the GDPR, adapted to meet the needs of the ADGM. They are intended to be proportionate and business friendly whilst still requiring a high level of protection for personal data.

1.7 Alignment of the guidance with UK ICO/EU EDPB guidance

To make compliance more streamlined for international businesses, we have taken the approach of aligning this Guidance with the GDPR guidance produced by the UK's Information Commissioner's Office and the EU's European Data Protection Board (EDPB).

1.8 Link to legislation

You can view the DPR 2021 here: https://adgmen.thomsonreuters.com/rulebook/data-protection-regulations

About the DPR 2021

1.9 Key changes in the DPR 2021

Key changes introduced in the DPR 2021 compared to the ADGM Data Protection Regulations 2015 include:

- ***Territorial scope*** – the DPR 2021 can apply to businesses outside the ADGM in certain circumstances.

- ***Data Protection Officers*** – in certain circumstances controllers and processors must appoint data protection officers.

- ***Data protection impact assessment*** – controllers which carry out high risk processing activities must perform data protection impact assessments in advance of such processing.

- ***Data subjects' rights*** – controllers must respond to requests from data subjects to exercise their rights within 2 months of receipt of the request.

- ***Exemptions*** – the DPR 2021 contain exemptions from the requirement to comply with requests from data subjects to exercise in specific circumstances.

- ***Data breach notification*** – controllers must notify the Commissioner of a data breach within 72 hours of becoming aware of it.

- ***Cross border transfers*** – the DPR 2021 contain revised grounds on which transfers of personal data may be made to other jurisdictions.

- ***"Appropriate policy documents"*** – in certain circumstances, when processing special categories of personal data, controllers must have an appropriate policy document in place.

- ***Fines*** – the Commissioner has the power to issue fines of up to $28 million for breaches of the DPR 2021.

1.10 How the DPR 2021 are set out

The DPR 2021 are divided into 8 parts:

- ***Part 1 – General provisions*** – (subject matter and objectives, material scope, territorial scope).

- ***Part 2 – Principles*** (principles of processing; lawfulness of processing; conditions for consent, processing special categories of personal data; processing that does not require identification; processing for archiving and research purposes).

- ***Part 3 – Rights of the data subject*** (transparent information, communication and modalities for the exercise of the rights of the data subject; information to be provided where the personal data is collected from the data subject; information to be provided where personal data has not been obtained from the data subject; right of access by the data subject; right to rectification; right to erasure; right to restriction of processing; notification obligation regarding rectification or erasure of personal data or restriction of processing; right to data portability; right to object; automated individual decision-making including profiling; restrictions).

- ***Part 4 – Controller and processor*** (responsibility of the controller; data protection by design and default; data protection fee; joint controllers; processor; processing under the authority of the controller or processor; records of processing activities; cooperation with the Commissioner of Data Protection; security of processing; cessation of processing; notification of a personal data breach to the Commissioner of Data Protection; notification of a personal data breach to the data subject; data protection impact assessment; designation of the data protection officer; position of the data protection officer; tasks of the data protection officer; codes of conduct; certification).

- ***Part 5 – Transfers of personal data outside of ADGM or to international organisations*** (general principle for transfers; transfers on the basis of an adequacy decision; transfers subject to appropriate safeguards; binding corporate rules; derogations for specific situations; data sharing with public authorities; international cooperation for the protection of personal data).

- ***Part 6 – Independent supervisory authority*** (Commissioner of Data Protection; independence; functions and obligations of the staff of the Commissioner of Data Protection; general powers; budget; accounts and audit; annual report).

- ***Part 7 – Fines and remedies*** (directions; general conditions for imposing administrative fines; fixed penalties for non-payment of the data protection fee or renewal fee; right to

lodge a complaint with the Commissioner of Data Protection; application to court; rights against a controller and/or processor).

- ***Part 8 – Final provisions*** (power of the Board to make rules; previously concluded agreements; definitions; repeal of Data Protection Regulations 2015; short title, scope and commencement).

2. KEY TERMS AND CONCEPTS

This paragraph 2 covers the following key terms and concepts used in connection with the DPR 2021: data protection; personal data; special categories of personal data; controller; processor; processing.

Data protection

2.1 What is data protection?

Data protection is the fair and proper use of information about people and is key to building trust between people and organisations. It's about treating people fairly and openly, recognising their right to have control over their own identity and their interactions with others, and striking a balance with the wider interests of society.

Good practice in data protection is important to ensure public trust in, engagement with, and support for, innovative uses of personal data in the public and private sectors. It also helps remove unnecessary barriers to trade and co-operation.

Personal data

2.2 What is/is not personal data?

- Personal data is any data relating to an identified natural person or identifiable natural person.

- In other words it means data which relates to a living individual who:

  a) can be identified or who is identifiable, directly from the information in question; or

  b) can be indirectly identified from that information in combination with other information.

- If personal data can be truly anonymised then the anonymised data is not subject to the DPR 2021.

- Information about a deceased person does not constitute personal data and therefore is not subject to the DPR 2021.

- Information about companies or public authorities is not personal data, however, information about individuals acting as sole traders, employees, partners and company directors would be.

2.3 When is an individual identified/identifiable?

- An individual is identified or identifiable if they can be distinguished from others. You do not need to know their name for a person to be identified/identifiable.

- Examples of identifiers include names, photographs, ID numbers, location data, a combination of significant criteria (e.g. age, occupation, place of residence), online identifiers (e.g. IP addresses and cookie identifiers) but there are many others.

2.4 Can an individual be identified directly from information?

- If you can distinguish an individual from others by looking just at information you have, this individual will be identified.

- This may mean the information you hold constitutes personal data.

Example:

"The security guard who works on the front desk of Building X on weekends."

You don't need to know a person's name to identify them. If you hold an identifier or combination of identifiers, this can be sufficient to identify an individual.

Example:

"Joebloggs@CompanyABC.com"

This corporate email address identifies the individual named Joe Bloggs who works at CompanyABC.

2.5 Can an individual be identified indirectly from information we hold, together with other available information?

- Even if you need additional information to be able to identify someone, they may still be identifiable.

- That additional information may be information you already hold, or it may be information that you need to obtain from another source.

Example:

All employees within your organisation are allocated an employee ID number. Taken in isolation, this number does not identify anyone. However, the organisation has lists of which employee has been allocated which number. The employee ID number, together with other information the organisation holds, allows the identification of an individual.

Example:

A business uses Wi-Fi analytics data to count the number of visitors per hour across different retail outlets. This involves the business processing the Media Access Control (MAC) addresses of mobile devices that broadcast probe requests to its public Wi-Fi hotspots. MAC addresses are intended to be unique to the device.

If an individual can be identified from that MAC address, or other information in the possession of the business, then the data is personal data.

Special categories of personal data

2.6 What are special categories of personal data?

Certain types of personal data, known as special categories or personal data, receive additional protection under the DPR 2021 because they are more sensitive. The DPR 2021 define 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; or
- personal data relating to **criminal convictions and offences or related security measures**.

You can only process special categories of personal data if one of the conditions set out in section 7(2) of the DPR 2021 applies. Further information on processing special categories of personal data can be found in paragraph 5 of this document (Lawful bases for processing/Special categories of personal data).

Controllers and Processors

2.7 Why is it important to know if an organisation is a controller or processor?

The DPR 2021 distinguishes between two types of organisation when it comes to processing personal data. It is important to understand whether an organisation is acting as a controller or as a processor because different rights and obligations apply to each one.

The majority of the obligations under the DPR 2021 apply to controllers. A smaller subset of obligations apply to processors.

2.8 What are controllers?

The DPR 2021 defines a controller as "the natural or legal person, public authority, agency or other body, which alone or jointly with others, determines the purposes and means of processing of personal data".

The key element of being a controller is the element of control. Controllers are the main decision makers about **how** personal data is processed, and the **purposes** for which it is processed.

The definition provides for situations where two or more organisations may jointly control the processing of personal data. In these circumstances the organisations would be "joint controllers" (see paragraphs 2.9 - 2.10 below). However, if two or more organisations process the same set of personal data but for different purposes, they will not be joint controllers. Instead they will be separate/independent controllers.

Example:

An insurer collects information from its customers and potential customers which it uses to calculate premiums, and to assess and manage claims made under its policies.

The insurer is a controller of its customers' personal data as it decides what personal data to collect and process; the purposes for which to use such personal data; and makes decisions affecting the data subjects as a result of its processing activities.

Example:

A business uses a law firm to provide legal advice. The law firm processes personal data of the business's customers in order to provide its services to the business. In this case, the law firm is a controller of the personal data it uses in providing its services. This is because it decides how it uses the data and determines the content of the advice it provides. It also has professional responsibilities in relation to the data e.g. obligations relating to confidentiality and record keeping which would mean it could not simply follow the business's instructions on these matters.

Joint Controllers

2.9 What are joint controllers?

Two or more controllers will be joint controllers where they jointly determine the purposes and means of processing. This means that they must decide the purposes and means of processing together and that they are processing the data for the same or shared purposes. Controllers will not be joint controllers if they are each processing the same pool of data for different purposes.

Example:

A law firm and an accountancy firm decide to put on a joint training event on a new law. Those who register for the event provide their personal data as part the registration which the two organisations use to send out details of the event and copies of materials after the session. Neither organisation uses the personal data for any other purpose.

The two organisations will be joint controllers of the attendees' data as they have jointly decided what data to collect and how to use it, and are processing it for shared purposes.

2.10 What obligations arise where organisations are joint controllers?

Joint controllers must decide between them how they will make sure that their obligations under the DPR 2021 are met. In particular they need to decide:

- who will provide **information to data subjects** (e.g. in the form of a privacy notice/policy) about how their personal data is being processed;
- who will be responsible for facilitating the **exercise of data subjects' rights**; and
- who will act as a **contact point for data subjects** in relation to the joint processing activities.

The DPR 2021 say that joint controllers must do these things by way of an arrangement between them. There is no legal requirement that this arrangement is in the form of a written agreement, although having a written agreement between joint controllers can be a good way of making sure that everyone understands the allocation of responsibilities.

The DPR 2021 also require the joint controllers to make the "essence of the arrangement" available to data subjects. In practice this means making sure data subjects understand how the joint controllers are processing their personal data and who is responsible for compliance with the obligations set out in the DPR 2021. This information is usually given to data subject in a privacy notice.

Regardless of how the joint controllers allocate responsibility for compliance with DPR 2021 obligations, each one will remain responsible for complying with all the obligations of controllers under the DPR 2021.

2.11 What are processors?

The DPR 2021 defines a processor as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

Processors act on behalf of, and only on the instructions of the controller. They do not decide how or why to process personal data and they do not use it for their own purposes.

Employees of a controller are not processors.

Example:

A financial services business uses a specialist provider of payroll systems to manage its payroll. The provider processes details of the financial services business's employees in order to run the salary payment process. The arrangement is subject to a written agreement between the parties which governs how the service is to be provided.

The payroll provider is a processor. Although it makes some decisions about the processing, e.g. the systems it uses to process the data, the overall control of the processing remains with the financial services business. The payroll provider only uses the personal data to provide this service to the client organisation, subject to the client organisation's instructions and does not decide how or why to process the personal data itself.

2.12 How to decide if your organisation is a controller or a processor

You need to consider your organisation's role and responsibilities in relation to the data you process. It is possible for an organisation to be a controller in relation to some processing activities and a processor in relation to others.

If you have overall control of the "how" and the "why" of the processing, you will be a controller.

If you only use data on another organisation's instructions and not for any purposes of your own, you are likely to be a processor.

You are likely to be a controller if:

- you decide to collect/process personal data;
- you decide what personal data to collect/process;
- you decide what individuals to collect personal data from/process personal data about;
- the data subjects are your employees;
- you exercise professional judgment in relation to the processing;
- you are making decisions about data subjects as part of the processing;
- you are processing data because you are required to do so by law or professional rules; or

- you have appointed other organisations (e.g. processors) to help with aspects of the processing.

You are likely to be a processor if:

- you are following another organisation's instructions in relation to your processing;
- you are providing a service to a customer and processing personal data as part of this service;
- you do not make decisions about things like:
  - what data you process;
  - the purposes for which you process the data;
  - what individuals' data you process;
  - how long you keep the data;
  - what lawful bases the processing relies upon; or
  - who the data is disclosed to.

Processing

2.13 What is processing?

The term "processing" is defined in the DPR 2021 as "any any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

This is a very wide definition and really encompasses anything which an organisation could do with personal data, including holding/storing it without actively using it for anything, or simply deleting it.

It should be noted that some laws may require you to process personal data for specific reasons, for example, registering information about company directors. Even though this may be a processing that is required by law, it still falls within the definition of "processing" and you should still consider whether the DPR 2021 applies.

3. SCOPE

Material Scope

3.1 When do the DPR 2021 apply?

The DPR 2021 apply to:

- the processing of personal data either wholly or partly by automated means; and
- the processing of personal data, other than by automated means, which forms part of or is intended to form part of a filing system.

The DPR 2021 do not apply to the processing of personal data:

- by a natural person for a purely personal or household activity; or
- by public authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences to the execution of criminal penalties, including safeguarding against and preventing threats to national security.

3.2 What is processing wholly or partly by automated means?

"Automated means" refers to data held in electronic form. The most obvious example is data held on a computer system.

3.3 What is a filing system?

A filing system is defined in the DPR 2021 as "any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis".

This means data held in manual form which is organised in a structured way, such that a person can find particular information by reference to a specific criteria. A good example of data which would fall within this definition is a set of paper-based records where the information is ordered alphabetically per customer.

Manual/paper records are only subject to the DPR 2021 if they are held or intended to be held in a filing system as described above.

Example:

A company keeps an archive of its email system going back over last 2 years. These are not structured/grouped in any way.

Although not structured/grouped, because the emails are held electronically, the storage of the personal data contained in them is subject to the DPR 2021.

Example:

The company has also printed out and retained certain emails. These are held in paper form in a filing cabinet but the emails are not grouped and the files not structured in any way.

These emails are not subject to the DPR 2021 because they are not processed by automated means and the files do not meet the definition of "filing system".

3.4 What is purely personal or household activity?

Personal data processed for a purely personal or household activity is not subject to the DPR 2021. This would include for example, maintaining an online address book with details of friends and family.

3.5 Territorial Scope

The DPR 2021 apply to "the processing of personal data in the context of the activities of an establishment of a controller or a processor in ADGM, regardless of whether the processing takes place in ADGM or not."

Example:

A business established in the ADGM also has a branch office in China. The branch office in China assists with managing the customer database and sending out marketing emails. Although this processing by the Chinese branch office does not take place in the ADGM, it happens "within the context of the activities" of the ADGM entity, and is therefore subject to the DPR 2021.

The location and nationality of the data subjects whose data is being processed is not relevant to the question of whether or not the DPR 2021 apply to any particular processing activity.

3.6 What is an establishment?

An establishment is any authority, body corporate, branch, representative office, institution entity, or project, which is established, registered or licensed to operate or conduct any activity within the ADGM.

3.7 What does "in the context of an establishment" mean?

The processing must take place in the context of the establishment of the controller or processor for the DPR 2021 to apply. This could include processing by entities which are outside the ADGM where their processing activities happen within the context of an ADGM establishment.

The two main factors which need to be considered when determining if processing is taking place within the context of an establishment in the ADGM are:

- *the relationship between the controller or processor outside the ADGM and its local establishment in the ADGM – if the processing activities of a non-ADGM controller or processor are inextricably linked to an establishment in the ADGM, the DPR 2021 may apply to such processing (even though the organisation doing the processing is outside the ADGM); and*

- *revenue raising within the ADGM* – if revenue raising in the ADGM by an ADGM establishment is inextricably linked to the processing of personal data taking place outside the ADGM, this may trigger the application of the DPR 2021 to the processing activities happening outside the ADGM.

Example:

An e-commerce website is operated by a US-based company which exclusively carries out the company's personal data processing activities. The company has an office in the ADGM which carries out marketing activities directed towards ADGM customers.

In this case, the activities of the ADGM office are inextricably linked to the processing of personal data carried out by the US e-commerce website as the marketing activities of the ADGM office are for the purpose of increasing sales on the US e-commerce website. The processing of personal data by the US company in relation to ADGM sales is inextricably linked to the activities of the ADGM office, and will therefore be subject to the DPR 2021.

3.8 When else might the DPR 2021 apply to processing taking place outside the ADGM?

It is not necessary for the processing itself to take place in the ADGM for the DPR 2021 to apply. A controller in the ADGM could for example, contract a processor in a location outside the ADGM where the actual processing takes place, and such processing would be subject to the DPR 2021.

In practical terms, this means the controller would need to comply with all the requirements of the DPR 2021 in respect of such processing, including requiring the processor to enter into a written contract with it which contains the terms set out in section 26 of the DPR 2021. You can find more details about controller-processor terms in paragraph 3 (Processors) of Part 3 of the Guidance.

3.9 Processors in the ADGM

Processors in the ADGM which are processing personal data for a controller which is outside of the ADGM must comply with the DPR 2021 to the extent possible, taking into account whether the controller is subject to similar obligations under the laws of its home jurisdiction.

In some cases, the processor will have full control over its own compliance with the DPR 2021 e.g. ensuring that it applies appropriate technical and organisational (security) measures to the personal data it processes, and notifying the controller if it suffers a personal data breach. However, in other circumstances the cooperation of the controller may be needed. A good example of this is the requirement that a processor which is established in the ADGM and subject to the DPR 2021 should enter into terms (set out in section 26 of the DPR 2021) with the controller to govern the processing being carried out.

The DPR 2021 recognise that it may not always be possible for a processor to comply with all requirements if the controller is not willing to cooperate.

Example:

A controller that is not registered in the ADGM uses a processor in the ADGM. The processor asks the controller to enter into a data processing agreement ("DPA") containing the terms required by section 26 of the DPR 2021.

The controller refuses to enter into the DPA on the basis that the laws of its own jurisdiction (which do not fall within the DPR 2021 definition of "applicable law") require it to enter into a DPA with a different set of terms.

4. PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

Section 4 of the DPR 2021 sets out 6 data processing principles. Controllers are responsible for making sure their processing complies with these principles and must be able to demonstrate this compliance.

4.1 Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

4.1.1 Lawfulness

For processing of personal data to be lawful, you need to identify a lawful basis for processing. The lawful bases for processing are set out in section 5(1) of the DPR 2021.

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.

If you cannot identify a lawful basis and, if relevant, an additional condition for processing special category personal data, you must not go ahead with the processing. More details on the lawful bases and conditions for special category personal data can be found in paragraph 5 (Legal bases for processing/special categories of personal data) of this document.

The lawfulness requirement also means that you must not do anything with the personal data which is unlawful in a more general sense e.g. because it breaches another law, duty owed by your organisation, or obligation in an enforceable contract.

4.1.2 Fairness

Processing data fairly means using it in a way that individuals would reasonably expect, and not in a way which produces unjustified negative effects on them.

Processing personal data fairly is closely linked to how you obtained the data in the first place and what you have told data subjects about how you will use their data (see paragraph 3 of Part 2 of this Guidance (Right to be informed)). If for example you have obtained data by deceiving or misleading people about how it will be used, this is likely to be unfair.

Example:

A shop asks for customers' email addresses which it tells them it will use to email a copy of their receipt.

As well as sending the receipts, the shop adds the email addresses to its marketing list and sends email marketing.

This is unfair as it has misled the customers about the use of their personal data.

4.1.3 Transparency

Transparency means being open, clear and honest with people about who you are, what you do with personal data and how/why you use personal data.

Transparency is particularly important at the start of your relationship with data subjects. If people understand how you want to use their data they can choose whether to enter a relationship with you. You must tell individuals how you are processing their data in a clear and easy to understand way. This also applies where you process the personal data of individuals you have no direct relationship with. You can find out more about transparency obligations and the information you must provide to people in Part 2 of the Guidance (Data subjects' rights).

4.2 Purpose Limitation

4.2.1 What is the purpose limitation principle?

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The purpose limitation principle means that you must be clear from the beginning why you are collecting personal data and how you intend to use it. Your transparency obligations mean you must tell people how and why you are processing their data.

You must specify your purposes in the privacy information you give to individuals, and also in your record of processing activities (unless your organisation is exempt). You can find out more about records of processing activities in Part 3 of the Guidance.

If you later want to use data in a way which is different or additional to the purposes you determined and communicated to people initially, you must be sure that the new use is fair, lawful and transparent. You can only go ahead if:

- the new purpose is compatible with the original one;
- you get the individual's consent to the new purpose; or
- a provision of law requires or allows the new processing.

When deciding whether a new purpose is compatible with your original purpose you should take into account:

- whether or not there is a link between your original purpose and the new purpose;
- the circumstances in which you originally collected the personal data. You should consider in particular what the data subjects would reasonably expect;
- the sensitivity of the personal data;
- how using the data for the new purpose will affect individuals; and
- whether you can carry out the new processing with appropriate safeguards in place e.g. encryption or pseudonymisation.

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 likely to be incompatible with your original purpose.

Example:

A person sets up a customer account with a business and in doing so, provides personal data to the company for this purpose. The company later shares the personal data with an airline so that the airline can send email marketing messages to the individual.

The disclosure of the personal data by the company to the airline for the purposes of the airline's marketing is incompatible with the original purpose for which the data was processed – i.e. opening a customer account.

4.2.2 Archiving and Research Purposes

The DPR 2021 say that if personal data is processed for Archiving and Research Purposes:

- the processing will be considered compatible with the initial purpose for which the personal data was collected; and
- the data may be stored for longer than the period stated in the storage limitation principle (section 4(1)(e)) of the DPR 2021 provided that appropriate steps are taken to safeguard the rights of the data subject.

The phrase "Archiving and Research Purposes" means:

- archiving purposes in the public interest;
- scientific or historical research purposes; or
- statistical purposes in accordance with section 9 of the DPR 2021.

Example:

An organisation is carrying out scientific research which involves using personal data which was originally required for a different purpose. Provided that the organisation complies with the safeguards set out in section 9 of the DPR 2021, this processing will not breach the purpose limitation principle.

Where data is processed for Archiving and Research Purposes, the safeguards set out in section 9 of the DPR 2021 must be applied.

4.3 Data Minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The data minimisation principle means:

- Making sure the data you are processing is **adequate** for the purpose you have identified. You may not be able to achieve your purpose if the data you have is insufficient.
- Making sure that the data you collect and process is **relevant** to achieving the purpose of your processing.
- Making sure that you are processing the **minimum** amount of data possible to achieve the specific purpose you have identified. In particular you should not collect and hold personal data on a speculative basis, just in case it may be useful in future.

Example:

A recruitment agency works with a number of different businesses. It tailors its candidate application form to make sure that it only requests personal data from each candidate that is relevant to the particular line of work they are interested in.

4.4 Accuracy

Personal data must be accurate and, where necessary kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

This means taking all reasonable steps to make sure the personal data you hold is correct and not misleading in any way. If you discover that it is, you must take all reasonable steps to correct it. You may also need to take steps to keep it up to date, although this will depend on the type of personal data you are processing and how you are using it.

Example:

A business needs to ensure it has up to date records of its employees' contact details and bank details so that it can communicate with them and pay their salaries. The business implements a self-service system so that employees can make their own changes to the records their employer holds about them. The business is taking steps to make sure that the personal data it holds is accurate and up to date.

You may hold personal data in the form of a record of opinion about a person. A record of an opinion is not necessarily inaccurate personal data just because the individual disagrees with it, or it is later proved to be wrong. It is important to ensure that you record that something is an opinion, and if appropriate, whose opinion it is. If you later become aware that the opinion is inaccurate, this should also be made clear in the records you hold. If a person challenges the accuracy of an opinion about them, you should record this challenge as well.

Individuals have the right to have inaccurate personal data rectified. You can find out more about the right to rectification in Part 2 of the Guidance (Data subjects' rights).

4.5 Storage Limitation

4.5.1 What is the storage limitation principle?

Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

This means that you need to think about how long you need to keep personal data to achieve the specific purpose for which it is processed. Once you have achieved this purpose, the data should be anonymised or securely deleted. It is recognised that it can be difficult to delete or erase all traces of data. The key point to bear in mind when seeking to delete data is to put it beyond use. If you delete personal data from live systems, you should also delete it from any back-ups of such system. Alternatively, you might choose to anonymise the data. Data is anonymised if it is in a form which does not permit identification of data subjects.

Example:

A business keeps records of its transactions with customers. It may be appropriate for the business to retain the records beyond the end of its relationship with its customers to help it deal with any customer complaints or claims.

Example:

A shopping centre uses CCTV for the purposes of security, and prevention/detection of crime. It retains footage for a period of 28 days, following which it is securely deleted. The centre considers that this is sufficient time for any incident to come to light. If an incident occurs that is captured by the CCTV, the relevant footage is retained for the duration of any investigation and proceedings.

The DPR 2021 do not set any maximum or minimum retention periods for personal data, although there may be other laws or guidelines applicable to you which do specify particular timeframes. It is up to you to determine the appropriate periods, taking into account your processing and any applicable legal requirements and professional guidelines. It is good practice to have a retention policy or schedule which lists the types of records and information you hold and allocates a retention period to each category. This can help you comply with the storage limitation principle.

4.5.2 Archiving and Research Purposes

Personal data which is processed for Archiving and Research Purposes (see paragraph 4.2.2 above) may be stored for longer periods than stated in the storage limitation period provided that appropriate technical and organisational measures are used to safeguard the rights of data subjects.

Appropriate safeguards could include for example, security measures to limit access to the data, or encrypting or pseudonymising the data.

4.6 Security

Personal data must be processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

For more information on data security please see the paragraph on Security of processing in Part 5 of the Guidance.

4.7 Accountability

Controllers are responsible for making sure their processing complies with the above principles and must be able to demonstrate this compliance. This is known as the accountability principle. It means that you need to take a proactive approach towards data protection and be able to evidence the steps you have taken to comply.

The accountability principle is linked to the requirement in section 22(1) of the DPR 2021 which requires controllers implement technical and organisational measures to ensure that their processing complies with DPR 2021 requirements, and to review and update those measures where necessary. It is important to be aware that complying with the DPR 2021 is not a one-off exercise but rather an ongoing process.

Where appropriate, taking into account the processing activities taking place, you will need to implement data protection policies as part of ensuring that your processing meets DPR 2021 requirements.

What will be appropriate in terms of accountably measures will depend on the size of your organisation, the sensitivity and amount of personal data you process and the purposes for which you use personal data.

Larger organisations which carry out significant processing may need to put in place a privacy management framework. This might include:

- robust program controls informed by the requirements of the DPR 2021;
- appropriate reporting structures; and
- assessment and evaluation procedures.

Smaller organisations may decide to approach accountability on a smaller scale and focus on things such as:

- ensuring that staff are aware of and understand their responsivities in relation to data protection;
- developing proportionate policies and procedures for handling personal data; and
- keeping records of what they are doing and why.

5. LAWFUL BASES FOR PROCESSING/ SPECIAL CATEGORIES OF PERSONAL DATA

5.1 Lawful bases for processing

To process any personal data you need to be able identify a relevant lawful basis for your processing. There are six lawful bases for processing which are set out in section 5(1) of the DPR 2021.

You must determine your lawful basis before processing and document this. You will also need to tell people what lawful basis you are using in your transparency information (e.g. your privacy notice). You should not swap between lawful bases once you have started processing unless you have a good reason for this.

If you are processing special category personal data you need to identify a lawful basis from the 6 below, and an additional condition for special category personal data (see paragraph 5.2 below).

Most lawful bases require that processing is 'necessary' for a specific purpose. This doesn't mean that the processing must be essential or the only way to achieve your purpose but if you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.

5.1.1 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 DPR 2021 set specific conditions for consent and if you do not meet these conditions, any consent you have obtained will be invalid.

Consent must be:

- ***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.

- ***Specific*** – specific consent means consent which relates to a particular processing activity/activities. The data subject needs to understand the purposes for which you intend to process their data before they are asked for or give consent. If you are 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.

- ***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.

- ***An unambiguous indication of the data subject's wishes given by way of a statement or clear, affirmative action*** – 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.

Example:

A business wants to be able to send marketing emails to customers. When customers 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.

If consent is given as part of a written declaration which also covers other things, the consent request to the processing of personal data must be separate and clearly distinguishable from the other matters. You must also use clear and plain language when requesting 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.

5.1.2 Performance of a 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).

Example:

A travel agent collects details from a customer about what kind of holiday they are looking for, the dates they want to travel, where they want to go and their name and contact details so they can suggest suitable options to the customer. The travel agent can process this personal data on the "performance of a contract" legal basis as the processing is necessary, at the request of the data subject, to take steps prior to entering a contract with the data subject.

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.

5.1.3 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.

"Applicable law" means any enactment or subordinate legislation applicable:

- in ADGM; or
- under Abu Dhabi or 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.

5.1.4 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 (see paragraph 5.2 of this document for further details).

5.1.5 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.

Applicable law has the same meaning as explained above in paragraph 5.1.3 above.

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.

5.1.6 Legitimate interest

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.

In this context "child" means a person under 18 and "third parties" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

The legitimate interest legal basis is the most flexible but this does not mean it will always be available for any processing you want to carry out. 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 ones which benefit society more widely.

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:

1. **Purpose test**: identify the relevant legitimate interest that you are pursuing:

    - 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?
    - What would the impact be if you couldn't go ahead?
    - Would your use of the data be unethical or unlawful in any way?

2. **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?

3. **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?

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.

If you process personal data on this basis you also need to tell individuals that you are doing so, and explain the nature of your legitimate interest. You can do this in the privacy information you give to people to meet your transparency obligations.

5.2 Special categories of personal data

The DPR 2021 define 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**; and
- 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 section 5(1) of DPR 2021, 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).

5.2.1 Explicit consent

You can process special category personal data if the data subject has given explicit consent to the processing for one or more specified purposes.

All the points made in paragraph 5.1.1 above in relation to consent will apply equally to explicit consent. The DPR 2021 do not define what is meant by explicit consent although explicit consent must be confirmed in words (including by way of a written statement) 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.

The above would be considered explicit consent.

5.2.2 Employment law

You can process special category 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 in accordance with section 7(3) of the DPR 2021.

This condition allows you to process special category personal data of employees where you are required or permitted to do so by law. If you rely on this condition you must be able to identify the relevant law which requires or permits the processing. Examples of processing activities which could be based on this condition include:

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.

Example:

An employer retains records of accidents and injuries that happen in the work place. The records contain data relating to health. The employer is required to maintain such records by laws relating to the health and safety of employees in the work place.

You will also need an appropriate policy document. See paragraph 5.3 below for further details.

5.2.3 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.

Although vital interests are not defined in the DPR 2021, these are intended to cover interests that are essential for someone's life, i.e. matters of life or death. This condition can only be relied upon where the data subject is physically or legally unable to give consent.

5.2.4 Health purposes

You can process special category personal data where necessary for health purposes, including:

- 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 health care systems or services; and
- pursuant to a contract with a health professional.

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.

The term health professional is not defined in the DPR 2021 but will include: doctors, nurses, midwives, dentists, opticians and optometrists, osteopaths, chiropractors, arts therapists, chiropodists, clinical scientists, dieticians, medical laboratory technicians, occupational therapists, orthoptists, paramedics, physiotherapists, prosthetists and orthotists, radiographers, speech and language therapists, pharmacists and pharmacy technicians and psychotherapists.

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.

5.2.5 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, health care needs, resources allocated to health care, the provision of and universal access to health care, health care expenditure and financing and the causes of mortality.

This condition is likely to be appropriate for processing which is necessary for: public health monitoring and statistics, public vaccination programmes, health care system resource planning, responding to threats to public health e.g. epidemics, clinical trials, regulatory approvals of drugs/medical devices, reviewing standards of clinical practice.

Example:

A manufacturer of medical devices maintains records of reports of problems/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.

5.2.6 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 (as defined in paragraph 5.1.3 of this document).

The phrase "Archiving and Research Purposes" means:

- archiving purposes in the public interest;
- scientific or historical research purposes; or
- statistical purposes in accordance with section 9 DPR 2021.

5.2.7 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 organisation as set out in its constitution or other similar document, and must not be unlawful or unethical in any way.

Nor do the DPR 2021 define what is meant by appropriate safeguards in this context, however, these are likely to be measures such as limiting access to the data, applying short retention periods, and providing individuals with the opportunity to opt out of processing.

5.2.8 Data made public by the data subject

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.

5.2.9 Performance of a contract

You can rely on this condition where processing is required:

- 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.

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.

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.

If the customer also wanted to add their spouse to the policy, the insurance provider could not rely on this condition to process details of the spouse's medical conditions as this person would not be a party to the contract.

5.2.10 Courts and legal claims

You can rely on this condition where the processing is necessary for the establishment, exercise or defence 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.

5.2.11 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. For more information on appropriate policy documents, see paragraph 5.3 below.

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.

5.3 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). You can find more details about these in paragraph 4 of this document; and
- your policies relating to retention and erasure of personal data. You can find out more about retention in paragraph 4 of this document, and about the right to erasure in Part 2 of the Guidance (Data Subjects Rights).

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 different 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 here: Appropriate Policy Document Guide and Template. Alternatively, you can access it through the Guidance Page of the Office of Data Protection website.

For more information, you may contact the Commissioner of Data Protection on:

Telephone No.: 00 971 2 3338888

Email: Data.Protection@adgm.com

Address: ADGM Building, Abu Dhabi Global Market Square, Al Maryah Island, Abu Dhabi, United Arab Emirates.

Disclaimer

This Guidance is a non-binding indicative Guidance and should be read together with the Data Protection Regulations 2021 and any other relevant regulations and enabling rules, which may change over time without notice. Information in this Guidance is not to be deemed, considered or relied upon as legal advice and should not be treated as a substitute for a specific advice concerning any individual situation. Any action taken upon the information provided in this Guidance is strictly at your own risk and the Office of Data Protection, Registration Authority and ADGM will not be liable for any losses and damages in connection with the use of or reliance on information provided in this Guidance. The Office of Data Protection, Registration Authority and ADGM make no representations as to the accuracy, completeness, correctness or suitability of any information provided in this Guidance.