ABU DHABI GLOBAL MARKET

Guidance on the Data Protection Regulations 2021

Part 3:

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

Office of Data Protection

TABLE OF CONTENTS

1. INTRODUCTION

Introduction to this Guidance

1.1 This is Part 3 in the series of guidance (Guidance) on the Abu Dhabi Global Market (ADGM) Data Protection Regulations 2021 (DPR 2021). This Part 3 covers the following topics:

- Data protection by design and by default (see paragraph 2);
- Data protection fee (see paragraph 3);
- Record of processing activities (see paragraph 4);
- Data Protection Officers (DPOs) (see paragraph 5); and
- Processors (see paragraph 6).

2. DATA PROTECTION BY DESIGN AND DEFAULT

2.1 What does the DPR 2021 require?

The DPR 2021 require that controllers must take appropriate steps to ensure that:

(a) their systems, business processes and practices in respect of which personal data is processed are designed taking into account compliance with the principles, rights and obligations in these Regulations (data protection by design); and

(b) only the processing of personal data that is necessary for each specific purpose of the processing is processed (data protection by default).

2.2 What is data protection by design?

Data protection by design is ultimately an approach that ensures you consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout its implementation and operation, including any updates or expansion and at its ultimate termination, closure or migration.

Ways in which data protection by design might be implemented include:

- putting in place appropriate technical and organisational measures designed to implement the data protection principles (paragraph 4 of Part 1 of the Guidance and section 9(1) of the DPR 2021) effectively. However, the DPR 2021 does not require the implementation of any specific technical and organisational measures; and
- building safeguards into your processing activities so that you meet the requirements of the DPR 2021 and protect individual rights. This will require you, at the outset, to consider the risks that your processing poses to the rights of individuals in the context of the nature and scope of the processing activities and then implementing appropriate measures accordingly.

Data protection by design has broad application and needs to be considered in a range of contexts. Examples include:

- developing or procuring new IT systems, services, products and processes that involve processing personal data;

- developing organisational policies, processes, business practices and/or strategies that have privacy implications;

- beginning to share personal data with a third party for a new purpose; or

- using personal data already processed within the organisation for new purposes.

2.3 What is data protection by default?

Data protection by default means that, by default, you only process personal data that is necessary to achieve your purpose. It ties back to the key data protection principles of data minimisation and purpose limitation (see paragraph 4 of Part 1 of the Guidance). It does not mean that the default settings in your system need to be set to collect no personal data.

You should consider things like:

- adopting a 'privacy-first' approach with any default settings of systems and applications. For example, if you use off-the-shelf software, you should carry out a risk assessment of the product and make sure that functions that do not have a legal basis or are not compatible with the intended purposes of processing are switched off;

- ensuring you do not provide an illusory choice to individuals relating to the data you will process. For example, if you do give individuals choice around where there personal data is stored, you should ensure that from a technical standpoint you implement that choice;

- ensuring that personal data is not automatically made publicly available to others unless the individual decides to make it so;

- implementing organisational measures supporting processing operations. Such measures should be designed so that only the minimum amount of personal data necessary for the specific process operations is collected and processed in each case. This would include ensuring that within the organisation there are measures in place so that only individuals which need personal data to perform their function have access to that personal data; and

- providing individuals with sufficient controls and options to exercise their rights.

2.4 Whose responsibility is it to ensure that data protection by design and default is implemented?

Section 23 of the DPR 2021 specifies that, as the controller, you have responsibility for complying with data protection by design and by default. This means taking an organisation wide approach to data privacy and embedding measures at all levels. For example:

- Your IT system architects. Those who design (or implement third party) systems, products and services should take account of data protection requirements and assist you in complying with your obligations. This should extend into contracts you have with any third party service providers that you use for your systems, or to support the delivery of your services and products. Please see paragraph 2.5 below; and

- Your senior management. Senior management in your organisation should take steps to foster a culture of 'privacy awareness' and ensuring you develop policies and procedures with the DPR 2021.

2.5 Do processors need to consider data protection by design and by default?

Section 23 of the DPR 2021 does not mention data processors specifically. However, section 26 of the DPR 2021 sets out the considerations you must take whenever you are choosing a processor. For example, you must only use processors that provide: "*sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of these Regulations and ensure the protection of the rights of the Data Subject*".

If, as a controller, you use a third party platform or system to process personal data on your behalf, you should choose one which enables you to meet your obligations under the DPR 2021. This would be a way in which you could take into account the principle of data protection by design.

Example:

You, as a data controller, are considering engaging a third party to provide a cloud based HR platform to store and manage personal data which relates to your employees.

One provider (Provider A) has designed their platform in such a way that the HR administrator within your organisation can easily control which other individuals within the organisation can see certain data types and which cannot, so that only those individuals which need access to employee personal data can see that personal data, and they can only see the personal data which they require to properly fulfil their function.

Another provider (Provider B) does not offer this flexibility and only offers an "all or nothing" setting whereby employees can either see all of their colleagues' personal data, or none at all.

Whilst not necessarily under a direct obligation under the DPR 2021 to ensure privacy by design, Provider A will support you in meeting your obligations under section 23 of the DPR 2021 and would be better placed to stand behind the contractual commitments, Provider A, as a Processor, is required to make under section 26(3) of the DPR 2021.

2.6 What does this mean, practically speaking?

One way of transforming the abstract concepts of data protection by design and default into reality is to implement a set of practical, actionable guidelines that individuals across your organisation can access and refer other stakeholders to.

Depending on the scale of your organisation and the resources available to you, as well as the risks associated with the processing activities you typically undertake, you might also run internal sessions explaining the concepts of data protection by design and default to key stakeholders in your organisation and encouraging them to collaborate to make these responsibilities part of their everyday roles. We would recommend framing any such discussion

in the context of the key principles set out at Part 2 of the DPR 2021 (see part 4 of Part 1 of the Guidance).

We recommend taking an organisation wide approach that seeks buy-in from key stakeholders and which focuses on realising clear outcomes, such as ensuring that:

- data protection issues are part of the design and implementation of systems, services, products and business practices;
- data protection is a fundamental component of the core functionality of your organisation's processing systems and services, rather than an afterthought;
- your organisation only processes the personal data that it needs in relation to its purposes(s), and that it only uses the data for those purposes;
- personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals (such as your employees or clients) should not have to actively take steps (such as adjusting settings or opting out) to protect their privacy;
- the identity and contact information of those primarily responsible for data protection compliance are available both within your organisation and to individuals whose personal data you process;
- you offer strong privacy defaults, user-friendly options and controls, and respect user preferences where those are offered.

Many of these practices relate to other obligations in the DPR 2021, such as transparency requirements, documentation, the role of DPOs and the use of data protection impact assessments (DPIAs). This is a reflection of the overarching and pervasive nature of the concepts of data protection by design and by default. By considering how you plan to meet those requirements at the outset of any new processing activity, you are embedding the principles of data protection by design and by default within your organisation.

Below are two further examples of how the principles of data protection by design and default might be implemented.

Example:

A controller is designing a privacy policy on their website in order to comply with the requirements of transparency. Using the principle of data protection by design to meet the key principle of transparency, the privacy policy should not contain overly lengthy or complex information that is difficult for the average data subject to digest and understand. It should be written in clear and concise language and make it easy for the user of the website to understand how their personal data is processed.

In an effort to design its privacy policy in the most user friendly way, the controller could provide the information in a layered manner, where the most important points are included in a list, with more detailed information being included in dropdown sections.

Another way in which the principle of data protection by design might impact the provision of privacy policy could be around the way in which it is made available to data subjects. This might mean making it readily available and clearly identifiable on the home page, rather than being accessible only by clicking through various sub-pages.

Example:

An insurance company wishes to use artificial intelligence (AI) to profile customers buying insurance as a basis for their decision making when calculating the associated insurance risk. At the stage at which the company is considering how their AI system will operate, it is determining the means of processing and should consider data protection by design when choosing an AI application from a supplier and when deciding on how to train the AI. Applying the concept of data protection by design, the company may decide to:

- ensure that it inputs accurate data to achieve precise results when training the AI system;
- pseudonymising personal data before inputting it into the system;
- regularly review the AI systems to mitigate against bias;
- put in place internal procedures to regularly review the analyses performed by the AI to check that it is performing well and adjusting the algorithm if it is not; and
- putting in place internal processes at the outset to ensure that the data subject's rights under section of the 20 of the DPR 2021 are upheld.

3. DATA PROTECTION FEE

3.1 What does the DPR 2021 require?

Section 24 of the DPR 2021 requires controllers to pay a data protection fee to the Commissioner of Data Protection before, or as soon as reasonably practicable after, they start processing personal data under the DPR 2021.

It is also necessary to provide the Commissioner of Data Protection with:

- name and address (which, in the case of a registered company, will be its registered office); and

- the date on which the controller commenced Processing Personal Data under the DPR 2021.

It is important to note that all licenced persons in the ADGM would have already provided the necessary information to the Commissioner of Data Protection during the company incorporation and registration process. The date of incorporation is also the date the controller may commence processing personal data, such as the personal data of directors, shareholders and other statutory role holders.

Each year, within one month of the expiry of the anniversary on which a controller commenced processing personal data under the DPR 20201 it is also necessary to pay the renewal fee.

3.2 How much is the data protection fee and the renewal fee?

The amounts payable are set out in the Data Protection Regulations 2021 (Fees) Rules 2021.

3.3 How do I pay the data protection fee?

You can pay through the Registration Authority's platform. Please note, all licensed persons would have already paid the initial data protection fee during incorporation and registration process. Your obligation is to ensure the yearly renewal fee is paid on time.

3.4 Will I be reminded to pay the renewal fee?

The Registration Authority's platform may send a reminder before the due date. However, it is your responsibility to ensure that you diarise the date on which the renewal fee is due.

3.5 What are the consequences of non-payment?

Failure to pay the data protection fee or the renewal fee can result in a fine of up to 150% of the data protection fee or the renewal fee (as applicable), as well as payment of the data protection fee or the renewal fee due.

Continued failure to pay the data protection fee (or the renewal fee) (as applicable) would lead to a debt being payable to the Commissioner of Data Protection. The Commissioner of Data Protection can apply to the ADGM Courts for recovery of the debt, plus such interest, costs of enforcement (including legal costs) and other expenses directly arising from the failure to pay as the ADGM Courts see fit to order.

4. RECORD OF PROCESSING ACTIVITIES

4.1 What does the DPR 2021 require?

As per section 28 of the DPR 2021 each controller and processor to which the DPR 2021 applies must maintain a record of processing activities in writing. This can be in electronic form, but it does not necessarily need to be.

The record of processing activities must be made available to the Commissioner of Data Protection upon request.

4.2 What does the record of processing activities need to include for controllers?

That record must contain a record of all processing activities under its responsibility:

- the name and contact details of the controller and, where applicable, the joint controller and the DPO;

- the purposes of the processing;

- a description of the categories of data subjects (e.g. employees, customer representatives, supplier representatives, third party advisors, etc.);

- a description of the categories of personal data (e.g. contact information, financial information, employment information, etc.). For ease of reference, it is recommended that categories of personal data are defined within the record so that it is clear the types of personal data which fall within those categories. This could be done by including a reference page with a key;

- the categories of recipients to whom the personal data has been, or will be disclosed including recipients outside of ADGM or in international organisations (as defined under the DPR 2021). Subject to the bullet point immediately below, it is not necessary to include reference to each individual recipient, provided that all recipients are caught within a category (e.g. "non-ADGM financial regulators"). However, if parties wish to name individual recipients, they certainly can elect to do so;

- where applicable, details of transfers of personal data outside of ADGM or to an international organisation, including the identification of that location outside of ADGM or the international organisation and, in the case of transfers referred to section 44(1)(b) of the DPR 2021, the documentation of suitable safeguards for each transfer. This includes where personal data is hosted by a third party on your behalf (e.g. A cloud service provider) and that third party hosts the data outside of the ADGM. For further details on international transfers, please refer to Part 4 of this Guidance (International Transfers);

- where possible, the envisaged time limits for erasure of the different categories of personal data. For example, it could be stated that personal data relating to employees is retained for [x] years following the termination of their employment; and

- where possible, a general description of the technical and organisational security measures referred to in section 30(1) of the DPR 2021. The Commissioner of Data Protection recognises that organisations may be reticent to disclose details of specific technical measures (i.e. cyber and infrastructure measures for internal security), in particular for financial institutions and those operating in the public sector. As such, a high level description of those would be sufficient.

4.3 What does the record of processing activities need to include for processors?

That record must contain a record of all categories of processing activities carried out on behalf of a controller, including:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting and the processor's DPO (if it has one);

- the categories of processing carried out on behalf of each controller. This means the types of things that you do with personal data, e.g. marketing, payroll processing, IT services, etc.;

- where applicable, details of transfers of personal data outside of ADGM or to an international organisation, including the identification of that location outside of ADGM or the international organisation and, in the case of transfers referred to section 44(1)(b) of the DPR 2021, the documentation of suitable safeguards; and

- where possible, a general description of the technical and organisational security measures referred to in section 30(1) of the DPR 2021.

4.4 What if you act in some capacity as a controller and some capacity as a processor?

Many organisations will act as both data processors and data controllers, depending upon the circumstances under which they are processing personal data. In order to meet the requirements of sections 28(1) and 28(2) of the DPR 2021, such organisations could either:

- have two separate records: one which covers their activities as a processor and once which covers their activities as a controller; or

- have one record which covers both, but which clearly distinguishes the capacity in which they are acting.

This will require organisations to have a clear understanding of the capacity in which they are processing data, which is useful in enabling them to ensure that they are meeting the relevant requirements under the DPR 2021.

Example:

You, as a payroll services provider act as processor for your customers' employee financial data, which you hold in order to be able to provide payroll services to your customers. You do not decide how that personal data is processed and you only process it upon the instructions of your customer.

However, as you also have your own employees you will be acting as a controller with respect to their personal data which is used for your own organisation's internal HR purposes.

4.5 Is there anything else which we can include?

As part of your record of processing activities, it can be useful to document (or link to documentation of) other aspects of your compliance with the DPR 2021. Such documentation may include:

- information required for privacy notices, such as:
    - the lawful basis for the processing
    - any legitimate interests for processing
    - the existence of automated decision-making, including profiling
    - the source of the personal data;

- records of consent;
- controller-processor contracts (as per section 26(3) of the DPR 2021);
- DPIA reports; and
- records of personal data breaches.

4.6 How do we go about creating a record of processing?

Doing an information audit or data-mapping exercise can help you find out what personal data your organisation holds and where it is held.

In the first instance, you can find out how personal data is used, who it is shared with (both internally and externally) and how long it is kept by distributing questionnaires to and / or holding workshops with relevant areas of your organisation and reviewing relevant policies, procedures and agreements.

You should see the creation of a record of processing as an opportunity to fully understand how data flows within your organisation, which may lead you to realise that certain personal data is in fact not necessary and should therefore not be processed at all, further to the necessity principle.

4.7 Is there a prescribed format for the record of processing?

No. Controllers and processors are free to develop a record of processing in any format they like, provided that it meets the requirements of the DPR 2021. We recommend that you develop a record which:

- is well structured;
- is digestible. It should be prepared in such a way that it can be readily understood by people with different areas of expertise (e.g. legal, finance, IT);
- is consistent in its use of terminology; and
- can be easily updated.

4.8 How often should our record of processing be updated?

Your record of processing should be a live document which reflects the data processing activities within your organisation. We would recommend diarising regular updates to ensure that it remains current and accurate. An annual update of the record will likely be insufficient. One method in which many organisations achieve this is by having data privacy champions in each area of the organisation which processes personal data, with that champion taking responsibility for liaising with stakeholders within their area or department.

There is always a risk that parts of your organisation may commence new processing activities without considering their data privacy implications and putting the necessary protections in place. If all employees are aware of and follow the principle of data protection by design, this shouldn't happen. However, ensuring that the record of processing is regularly updated will mean that there is transparency within the organisation around data processing activities so

that, in the event a new processing activity is commenced without sufficient consideration, this can be promptly identified and appropriate remediation action can be taken.

Whether one individual is responsible for centrally updating your record of processing, or whether a number of individuals are (e.g. the privacy champions) is a decision for each organisation to make and will depend upon the size of the organisation and the extent of its data processing activities. We would however recommend that someone in the organisation takes responsibility for monitoring the document as a whole, to ensure that the record remains consistent in terms of quality, level of detail and consistency of terminology.

5. DATA PROTECTION OFFICERS

5.1 What does the DPR 2021 require?

Controllers and processors must appoint a DPO where:

- the processing is carried out by a public authority, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, scope and purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data.

5.2 What is meant by "core activities"?

Your core activities are the primary business activities of your organisation. So, if you need to process personal data to achieve your key objectives, this is a core activity. This is different to processing personal data for other purposes, which are incidental to your business, but which is not part of carrying out your primary goals.

Example:

A recruitment agency may process candidate data on a regular basis to support them in improving their CV, preparing them for interview and putting them forward for suitable roles. The recruitment agency's processing of candidate data would be part of their core activities.

By contrast, a large bank with an internal recruitment team may also regularly process candidate data to fill internal vacancies, but that processing would not be part of its core activities. Rather, it would be ancillary to its core purpose (providing financial services to its customers).

5.3 What is meant by "regular and systematic monitoring of data subjects on a large scale"?

Neither "regular and systematic monitoring" nor "large scale" are defined under the DPR 2021.

However, the Commissioner of Data Protection is of the view that "regular and systematic" monitoring of data subjects includes all forms of tracking and profiling, both online and offline.

When determining if processing is on a large scale, you should take the following factors into consideration:

- the numbers of data subjects concerned;
- the volume of personal data being processed;
- the range of different data items being processed;
- the geographical extent of the activity; and
- the duration or permanence of the processing activity.

Example:

A large retail bank's website uses algorithms to monitor the searches and purchases of its customers and, based on this information, it offers recommendations for financial products to them. As this takes place continuously and according to predefined criteria, it can be considered as regular and systematic monitoring of data subjects on a large scale.

5.4 What does processing on a large scale of special categories of personal data mean?

When determining if processing of special categories of Personal Data is on a large scale in this context, you should again take the following factors into consideration:

- the numbers of data subjects concerned;
- the volume of personal data being processed;
- the range of different data items being processed;
- the geographical extent of the activity; and
- the duration or permanence of the processing activity.

Example:

A large retail insurance provider collects medical information relating to its customers or their employees (the insured) for the purpose of processing insurance claims and / or calculating premiums.

5.5 Can a single DPO be appointed for a group?

Yes. A DPO can be appointed in respect of a single entity, a group or multiple, independent entities.

If your DPO covers several organisations (or regions within your group), they must still be able to perform their tasks effectively, taking into account the structure and size of those organisations. This means you should consider carefully if one DPO can realistically cover a broad range of geographical areas or a particularly complex collection of organisations which have a range of different processing activities.

It is the responsibility of the controller and / or processor who appoints the DPO to ensure that the DPO receives the necessary support to perform their role effectively.

5.6 Can the DPO be an employee with another role within the organisation?

Yes. The DPO can also perform other roles within the organisation, however, it is key that the DPO must be able to perform his or her role in accordance with the DPR 2021 and must not hold another role which conflicts or is likely to conflict with his or her obligations under the DPR 2021.

Example:

A technology company's head of growth is tasked with increasing user numbers by driving users to take certain actions within the organisations mobile application. This person could not also act as the DPO as the decision making involved is likely to lead to a conflict of interest.

5.7 Does the DPO need to be an employee?

No. The DPO does not necessarily need to be an employee, provided that he or she operates under a written agreement with your organisation (i.e. a service contract).

5.8 Does the DPO need to be located in the ADGM?

The DPO also does not need to be a resident in the ADGM, but must be easily accessible to employees of your organisation, the Commissioner of Data Protection and data subjects whose personal data is processed by your organisation. Where an organisation makes regular use of online technology (e.g. Video calling tools) to communicate, this may be sufficient to meet the ease of accessibility requirement, provided that the DPO is genuinely accessible via such technologies. The DPO's contact details should be included in all of your privacy notices, as well as in your record of processing.

5.9 Does the DPO need to have any particular qualifications?

The DPR 2021 says that you should appoint a DPO on the basis of their professional qualities, and in particular, expert knowledge of data protection law.

It doesn't specify the precise credentials or qualifications that DPOs are expected to have, but the Commissioner of Data Protection recommends that the DPO's level of experience and knowledge should reflect the risk associated with the type of processing being carried out by the organisation.

So, where your organisation is processing data in a particularly risky or complex way, your DPO should be capable of understanding those processing activities and be confident to provide adequate oversight. It is also useful if the DPO has a strong understanding of the sector in which your organisation operates and the types of data processing typically associated with it.

The Commissioner of Data Protection has the power to approve certifications. This may include demonstrating the 'expert knowledge of data protection law' requirement of appointing a DPO. Whilst the certification will be attributable to the Data Controller or Processor, it will also demonstrate the individual as having the required expertise in and knowledge of data protection law.

5.10 Do we need to notify the Commissioner of Data Protection?

Yes. The controller or the processor must notify the Commissioner of Data Protection within one month following the appointment or resignation of any DPO. The notification must include the contact details of the new DPO and, in the case of a resignation, reasons for the resignation. You can update or provide information regarding the appointment and cessation through the Registry Platform.

The DPO's contact details must also be provided to the Commissioner of Data Protection where:

- notifying it of a data breach; and
- notifying the Commissioner of Data Protection of a DPIA which would be likely to result in a high risk to data subjects.

5.11 What support do controllers and processors need to provide to DPOs?

Controllers and processors must ensure that the DPO:

- is involved, properly and in a timely manner, in all issues which relate to the protection of Personal Data. This means it is important that all key stakeholders are introduced to and understand the DPO's role and seek his or her input in a meaningful way at a point in time where his or her recommendations can be taken on board and actioned appropriately;

- is provided with sufficient resources, access to personal data and processing operations to carry out the role. All stakeholders who are involved in processing activities should be ready and willing to support the DPO and to take on board his or her recommendations;

- is not dismissed or penalised for performing the tasks assigned to it under the DPR 2021. The DPO should be free to perform his or her role effectively without fear of recourse; and

- reports directly to the highest level of management in the organisation. This doesn't mean that the DPO's day to day activities need necessarily be managed by the highest level of management, but rather that they have access to and provide feedback and advice directly to those individuals.

5.12 Confidentiality

The DPO must be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with applicable law and the confidentiality policies and procedures of the controller or processor.

5.13 What does the DPO need to do?

The DPO must:

- inform and advise the controller or the processor and the employees who carry out processing of their obligations under the DPR 2021 and to other data protection provisions under applicable ADGM, Abu Dhabi or Federal UAE law. This may be through developing and circulating internal guidance material and would also ideally include running training sessions;

- monitor compliance with:

    - the DPR 2021, with other data protection provisions under the DPR 2021;
    - other data protection provisions under applicable ADGM, Abu Dhabi or Federal UAE law; and
    - the policies of the controller or processor in relation to the protection of personal data;

- provide advice around DPIAs and carry out reviews of processing activities which were subject to DPIAs. It is imperative that stakeholders are made aware (through appropriate internal training and communications) that they must inform the DPO whenever commencing a new processing activity that is likely to result in a high risk to the rights of data subjects; and

- cooperate with the Commissioner of Data Protection and to act as the contact point for the Commissioner of Data Protection on issues relating to processing and to consult with the Commissioner of Data Protection, where appropriate, with regard to any other matter.

5.14 Can the DPO be assigned other tasks?

Yes, provided that those do not conflict with the DPO's responsibility under the DPR 2021. For example, the DPO may well take the lead on maintaining the record of processing.

5.15 Does the DPO take on any personal liability?

No. Controllers and processor are ultimately liable for their compliance with the DPR 2021. However, it is important that you select an appropriate DPO to support you in meeting your compliance obligations.

6. PROCESSORS

6.1 What are processors?

As set out in paragraph 2.12 of Part 1 of this Guidance, 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; and
- 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.

6.2 Contracts with processors

Whenever a controller uses a processor, there must be a written contract (or other legal act) in place.
The contract is important so that both parties understand their responsibilities and liabilities with respect to the personal data being processed by the processor on behalf of the controller.

If a processor uses another organisation (i.e. a sub-processor) to assist in its processing of personal data for a controller, it needs to have a written contract in place with that sub-processor.

The DPR 2021 sets out what needs to be included in the contract.

- the subject matter of the processing;
- the duration of the processing;
- the nature and purpose of the processing;
- the type of personal data involved;
- the categories of data subject; and
- the controller's obligations and rights.

The contract or other legal act must also include terms or clauses stating that:

- the processor must only act on the controller's documented instructions (including with regards to transfers of personal data from the ADGM), unless required by appliable (ADGM, Abu Dhabi or Federal UAE) law to act without such instructions (in which case it

must inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

- the processor must ensure that people processing the data are subject to a duty of confidence (either contractually or under appliable (ADGM, Abu Dhabi or Federal UAE) law);

- the processor must take appropriate measures to ensure the security of processing (as per Section 30 of the DPR 2021);

- the processor must only engage a sub-processor with the controller's prior authorisation and under a written contract (see paragraph 6.5 below);

- the processor must take appropriate measures to help the controller respond to requests from individuals to exercise their rights;

- taking into account the nature of processing and the information available, the processor must assist the controller in meeting its obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;

- the processor must delete or return all personal data to the controller (at the controller's choice) at the end of the contract, and the processor must also delete existing personal data unless the law requires its storage; and

- the processor must submit to audits and inspections. The processor must also give the controller whatever information it needs to ensure they are both meeting their section 26 obligations.

Please check the ADGM website for the standard clauses which meet these requirements published by the Commissioner for Data Protection. The standard clauses are a template only and it is still necessary to include the particulars of processing for those to meet the requirements of the DPR 2021.

It is not necessary to use the standard clauses published by the Commissioner for Data Protection, provided that the contract meets the requirements set out above.

6.3 What responsibilities and liabilities do controllers have when using a processor?

Controllers must only use processors that can give sufficient guarantees they will implement appropriate technical and organisational measures to ensure their processing will meet DPR 2021 requirements and protect data subjects' rights.

Controllers are primarily responsible for overall compliance with the DPR 2021, and for demonstrating that compliance. If this isn't achieved, they may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

6.4 What responsibilities and liabilities do processors have in their own right?

In addition to its contractual obligations to the controller, a processor has some direct responsibilities under the DPR 2021. If a processor fails to meet its obligations, or acts outside or against the controller's instructions, it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

6.5 Sub-processors

A processor may not engage a sub-processor's services without the controller's prior specific or general written authorisation. If authorisation is given, the processor must put in place a contract with the sub-processor. The terms of the contract that relate to those elements listed at paragraph 6.2 above must offer an equivalent level of protection for the personal data as those in the contract between the controller and processor. Processors remain liable to the controller for the compliance of any sub-processors they engage.

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