ABU DHABI GLOBAL MARKET

Guidance on the Data Protection Regulations 2021

Part 5:

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

Office of Data Protection

TABLE OF CONTENTS

1. INTRODUCTION

Introduction to this guidance

1.1 This is Part 5 in the series of guidance (Guidance) on the Abu Dhabi Global Market (ADGM) Data Protection Regulations 2021 (DPR 2021). It covers the following topics:

- Security of processing;
- Cessation of processing; and
- Personal data breach notifications.

2. SECURITY OF PROCESSING

2.1 What security obligations do we have?

The obligation to provide appropriate technical and organisational (security) measures for personal data applies to both controllers and processors.

The DPR 2021 do not specify any particular security measures, rather it is up to the organisation to judge what is appropriate in the circumstances taking into account:

- the state of the art (i.e. the current state of technological development as appropriate to the context including: industry practice; the type and scale of the processing; and the availability of a product or solution in the market);
- the costs of implementation;
- the nature, scope, context and purposes of the processing; and
- the likelihood and severity of risks to data subjects' rights (in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data).

2.2 What security measures should we use?

Whilst the DPR 2021 do not set out any mandatory measures, they do give examples of the types of security measures which organisations should consider:

- ***Pseudonymisation and encryption***:
  - ***Pseudonymisation*** means processing personal data in such a way that the data can no longer be linked to a specific individual without the use of additional information which is kept separately and subject to security measures. Pseudonymised data is still subject to the DPR 2021.

Example:

An ADGM organisation gives each member an ID number. The list of which member maps to which ID number is held separately and subject to appropriate security measures.

The list of IDs can be considered pseudonymised data since it cannot be linked to a specific individual without the use of the separate list of names and IDs.

- ***Encryption*** is the process of using a secret value or key to encode data so that only others with access to that value/key are able to read the information. The two main purposes for which organisations generally use encryption are data storage and data transfer. Encrypted data is still subject to the DPR 2021.

- The ability to ensure the ongoing ***confidentiality, integrity, availability and resilience*** of processing systems and services.
  - ***Confidentiality*** means ensuring that only authorised people have access to/can view the data.
  - ***Integrity*** means ensuring that data is protected from unauthorised changes so that it is reliable and correct.
  - ***Availability*** means ensuring that authorised users have access to the data as needed.
  - ***Resilience*** means ensuring that your systems can continue to operate under adverse conditions such as a physical or technical incident, and being able to restore them to an effective state.

- The ability to ***restore the availability and access to personal*** data in a timely manner in the event of a physical or technical incident.

Example:

A business suffers a system failure which means it is unable to access any stored data. The organisation has an appropriate backup process in place where data is backed up to an offsite server every 24 hours. This means that it is able to restore the data a timely manner.

- A process for ***regularly testing, assessing and evaluating the effectiveness*** of technical and organisational measures for ensuring the security of the processing.
  - Exactly how you do this will depend on the nature of the organisation and the data processed.
  - A number of techniques such as vulnerability scanning and penetration testing may be helpful.

- You should document the results of the testing, assessment and evaluation process and any changes you make as a result.

2.3 What are technical measures?

Section 30(1) of the DPR 2021 requires controllers and processors to provide "appropriate technical and organisational measures". Technical measures encompass physical security measures and IT/cybersecurity measures.

Examples of ***physical security*** measures include:

- The quality of doors and locks and your premises, and use of alarms, security lighting, CCTV, security guards etc.;
- Access control to your premises, both in relation to your own staff and visitors;
- Disposal of paper and electronic materials; and
- How you keep IT equipment such as computers, laptops, mobile phones etc. secure.

Examples of ***IT/cybersecurity*** measures include:

- System security – the security of your network and information systems;
- Data security – the security of the data you hold, in particular the access controls which are applied;
- Online security – the security of your website and other online applications and services; and
- Device security – the security measures applied to devices such as laptops and mobile phones.

2.4 What are organisational measures?

Examples of ***organisational*** measures include:

- Carrying out an information risk assessment – this might involve:
  - reviewing the personal data you hold and considering how valuable/sensitive it is and the likely risks that could result if the data was compromised;
  - taking into account the nature and extent of your organisation's premises and systems;
  - assessing the number of staff you have and their access to personal data; or
  - the processing carried out on your behalf by any processors/sub-processors.
- Appointing a person within the organisation who has day to day responsibility for information security and ensuring that the person has the skills and resources to fulfil this role.

- Building a culture of security awareness in your organisation e.g. via regular training and awareness-raising campaigns.

- Developing an information security policy.

2.5 Individuals acting under the authority of controller/processors

The DPR 2021 say that controllers and processors must take steps to make sure that anyone acting under their authority (such as employees, contractors, temporary workers etc.) who has access to personal data only processes that data on the controller's instructions, unless they are required to process the data by applicable law (as defined below).

This means that you must make sure your staff understand the importance of data protection. You should provide regular training covering points such as:

- The responsibilities of your organisation as controller or processor under the DPR 2021 ;

- Staff responsibilities for protecting personal data, including that they must not access or disclose personal data without your authority; and

- The dangers of people trying to obtain personal data from them by deception, e.g. by pretending to be the data subject, or claiming to have an official reason to be given the data.

Example:

A controller sets access controls to its customer data using the principle of least privilege (i.e. staff are given the minimum access permissions needed to perform their roles). As well as this, staff are provided with training on data protection and data security when they first join the business and are required to complete refresher training on an annual basis.

"**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.

3. CESSATION OF PROCESSING

3.1 When must we cease processing?

When one of the following happens:

- your lawful basis for processing can no longer be relied upon; or

- the data subject exercises their right to erasure and none of the criteria from section 15(3) of the DPR 2021 applies (see Part 2 of the Guidance – (Data Subject Rights) for more information on the right to erasure),

you must:

- securely and permanently delete the personal data;
- anonymise the data so that it is no longer personal data and no data subject can be identified from it;
- pseudonymise the personal data; or
- securely encrypt the personal data.

Example:

An organisation is processing its customers' personal data on the legal basis of consent. A customer withdraws consent to the processing and the organisation has no other legal basis. It decides to securely and permanently delete the customer's personal data.

3.2 What if it is impossible to permanently delete, anonymise, pseudonymise or encrypt the data?

If you cannot securely and permanently delete, anonymise, pseudonymise or securely encrypt the data, you must archive it in a way which puts it beyond further use.

It is recognised that permanently deleting all copies of personal data from a system is not always straight forward. If that is the case, and the other options described above are not possible or appropriate you can instead put the data beyond use. This means that:

- the controller and any relevant processor are unable to use the personal data in any way to inform any decision about the data subjects, or in any other way which could affect the data subjects (although the data can be across checked by automated means solely to prevent further processing of personal data relating to the data subject);
- no party has access to the data apart from the controller and any relevant processor;
- the data is protected with appropriate technical and organisational security measures equivalent to those afforded to live data; and
- the controller and any relevant processor have in place and comply with, a strategy for permanent deletion, anonymisation, pseudonymisation or secure encryption of the personal data. The controller and any relevant processor must comply with such strategy and be able to demonstrate such compliance.

Provided the above four steps are followed, you would not be expected to include any data put beyond use in a response to a data subject access request although it may need to be produced in response to a court order.

3.3 Are there any exceptions?

The obligation to permanently delete, anonymise, pseudonymise or securely encrypt personal data does not apply where the personal data is:

- necessary for the establishment or defence of legal claims, or must be retained for compliance with applicable law (see defined term in para 2.5 above);
- being used in scientific research activity conducted in the public interest or in the interests of the ADGM in accordance with applicable laws and in a way which does not present risks to the rights of data subjects; or
- part of a dataset used to lawfully train or refine an artificial intelligence system in a manner that does not present risks to a data subject's rights.

If you rely on one of the exceptions you must have a policy and process for managing the relevant personal data when the exception no longer applies, at which point you must permanently delete, anonymise, pseudonymise or securely encrypt the personal data.

If you want to rely on the 2nd or 3rd bullets above, you must first carry out a data protection impact assessment (see Part 4 of the Guidance – Data Protection Impact Assessments) for more information on this topic).

4. PERSONAL DATA BREACH NOTIFICATIONS

4.1 What is a personal data breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

A personal data breach will have occurred whenever:

- any personal data is accidentally lost, destroyed, corrupted or disclosed;
- someone accesses the data or passes it on without proper authorisation; or
- data is made unavailable and this unavailability has a significant negative effect on individuals.

Example:

An organisation offers an online shopping service. It suffers a cyber-attack in which the attackers exfiltrate personal data of its customers.

Example:

The HR department of an organisation accidentally sends employee payslips to the wrong employees.

4.2 What breaches must be notified to the Commissioner of Data Protection?

You must notify the Commissioner of personal data breaches unless the breach is unlikely to result in a risk to the rights of individuals. When you discover a breach you must assess all the circumstances of the incident and establish the likelihood of the risk to the affected individuals. If a risk is possible you must report the breach to the Commissioner. If a risk is unlikely, you do not have to. If you decide the breach does not need to be reported you should keep a record of this decision so you are able to justify it if required.

Example:

An organisation offers an online shopping service. It suffers a cyber-attack in which the attackers exfiltrate personal data of its customers. When the organisation becomes aware of the incident it carries out an assessment of the likely risk to individuals.

The incident could result in the individuals suffering financial loss or identity theft and therefore the breach must be notified to the Commissioner.

Example:

A business sends out a promotional email to a group of customers offering a discount on clothing. The person sending the email forgets to use the bcc function so the email addresses of the recipients are visible to all who receive the email. When the organisation becomes aware of the incident it carries out an assessment of the likely risk to individuals.

The business concludes that the incident is unlikely to result a risk to the individuals. The product being advertised is not sensitive in any way and the potential for misuse of the customer email addresses in a way that creates a risk for individuals is limited. The breach does not need to be notified to the Commissioner but should be added to the business's internal data breach record.

4.3 What is the timeframe in which we must make the notification?

Notifications to the Commissioner must be made without undue delay, and within 72 hours of discovering the breach where feasible. If you are not able to report the breach within 72 hours you must explain why this is when you do report the breach.

If you do not have all the information that must be contained within a report within the first 72 hours, you can make an initial notification within the 72 hour period and then submit further information as it becomes available.

4.4 What information must be included in the notification?

The notification must include the following information:

- a ***description of the nature of the breach*** including:

- categories and approximate numbers of data subjects concerned;
- categories and approximate numbers of personal data records concerned;

- the ***name and contact details of your data protection officer*** or other contact person who can provide more information;
- the ***likely consequences*** of the breach; and
- a ***description of the measures taken*** or proposed to be taken to address the breach, including measures to mitigate its possible adverse effects if appropriate.

4.5 How do we notify the Commissioner?

You can report a breach via the Online Registry Solution. You must have authority over the entity on the system in order to report the breach. You can find more information about how to notify a data breach here: https://www.adgm.com/operating-in-adgm/office-of-data-protection/data-breach-notifications

4.6 When must we notify data subjects of breaches?

If a breach is likely to result in a high risk to the rights of individuals (unless one of the conditions below applies), you must tell the affected individuals without undue delay. Your notification must be written in clear and plain language and include the following information:

- a ***description of the nature of the breach***;
- the ***name and contact details of your data protection officer*** or other contact person who can provide more information;
- the ***likely consequences*** of the breach;
- a ***description of the measures taken*** or proposed to be taken to address the breach, including measures to mitigate its possible adverse effects if appropriate;
- where practical, ***recommendations for how the individual can mitigate potential adverse effects*** of the breach with sufficient detail to allow him/her to take the necessary precautions.

Practical mitigation recommendations might include things like:

- Changing passwords;
- Giving advice on how to select strong passwords;
- Reminding individuals to be vigilant for phishing emails; and

- Advising individuals to regularly check bank accounts for fraudulent activity.

Example:

An organisation offers an online shopping service. It suffers a cyber attack in which the attackers exfiltrate personal data of its customers.

When the organisation becomes aware of the incident it carries out an assessment of the likely risk to individuals. It determines that due to the nature of the data there is a high risk of incident resulting in the individuals suffering financial loss or identity theft.

It therefore notifies the individuals of the breach and makes recommendations on password changes and extra monitoring of bank accounts.

The DPR 2021 says that if one of the following conditions applies you do not need to notify individuals:

- You have implemented appropriate technical and organisation protection measures, and those measures were applied to the personal data affected, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption.

- You have taken subsequent measures which ensure that the high risk to the rights of data subjects is no longer likely to materialise.

- It would involve disproportionate effort (having regard to the number of data subjects, the age of the data and any appropriate safeguards adopted). In this case you must instead provide a public communication or similar measure to inform data subjects in an equally effective manner.

4.7 Documenting personal data breaches

You must document all data breaches, regardless of whether or not you notify the Commissioner of them. This record must contain:

- The ***facts*** relating to the breach;

- The ***effects*** of the breach; and

- The ***remedial action*** taken.

The record must contain all necessary information to enable the Commissioner of Data Protection to verify your compliance with the rules around breach notification. It is therefore good practice to include details of your assessment of the likely risks of the incident and an explanation of any decision not to notify the Commissioner of the breach.

4.8 Do processors have to notify breaches?

Processors must notify the controller whose personal data they are processing without undue delay once they become aware of the breach. Processors are not required to make notifications to the Commissioner or to data subjects.

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.