ABU DHABI GLOBAL MARKET

Guidance on the Data Protection Regulations 2021

Part 4: Data Protection Impact Assessments

Office of Data Protection

TABLE OF CONTENTS

1. INTRODUCTION

Introduction to this Guidance

1.1 This is Part 4 in the series of guidance (Guidance) on the Abu Dhabi Global Market (ADGM) Data Protection Regulations 2021 (DPR 2021). It covers when a Data Protection Impact Assessment (DPIA) should occur, what should be covered in a DPIA.

2. WHAT IS A DATA PROTECTION IMPACT ASSESSMENT?

A Data Protection Impact Assessment, or a DPIA for short, is a tool by which a controller can assess the risks to personal data that may be caused by implementing a particular process, operation or service that processes that personal data, and then identifying steps to mitigate against these risks.

More details about what must specifically be done when performing a DPIA are described in paragraph 4 below.

3. CONTROLLER'S OBLIGATIONS

3.1 What are the controller's obligations regarding DPIAs?

Per section 34(1) of the DPR 2021 a controller must, prior to processing that is likely to result in a high risk to the rights of natural persons, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

Per section 31(5) of the DPR 2021, a DPIA must also be used where the controller is seeking to rely upon one of the exceptions to a requirement for it to securely and permanently delete, anonymise, pseudonymise or encrypt personal data or put it beyond further use[1] because:

- the data is being used in scientific research activity conducted in the public interest or in the interests of the ADGM in accordance with the laws of the ADGM (or any Abu Dhabi or UAE Federal laws which apply in the ADGM), in a manner that does not present risks to the rights of data subjects; or

- is 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.

3.2 What is a "high risk to the rights of natural persons"?

There is no definition of what constitutes a "high risk to the rights of natural persons" in the DPR 2021, however risk in this context is about the potential for any significant physical, material or non-material harm to individuals.

The term "risk" implies a "more than remote chance" of some harm. "High risk" implies a higher degree or threshold of risk, either because the harm is more likely, or the potential harm is more severe, or a combination of both.

The question for such initial screening purposes is whether the processing is of a type likely to result in a high risk.

[1] Per section 31 of the DPR 2021, where processing is required to stop because the basis for processing has changed or ceases to exist, or where a data subject has exercised her or his rights under section 15 of the DPR 2021, and the controller must ensure that all personal data is (a) securely and permanently deleted; (b) anonymised so that the data is no longer personal data and no data subject can be identified form the data including where the data is lost, damaged or accidentally released; (c) pseudonymised; or (d) securely encrypted, unless one of the exceptions referred to here (amongst others) apply. These are the only exceptions listed at section 31 of the DPR 2021 that require a DPIA to be conducted.

3.3 When is processing "likely to result in a high risk to the rights of natural persons"?

There is no definition of "likely to result in high risk". However this should be considered as a more high-level screening test i.e., are there features in the proposed process, operation, plan or service that point to the potential for high risk? Here the controller is screening for any red flags which indicate that it needs to do a DPIA to look at the risk (including the likelihood and severity of potential harm) in more detail.

3.4 Other occasions when a DPIA may be useful

Although the DPR 2021 has specific obligations about when a DPIA must be conducted, it is also considered best practice to use DPIAs prior to the launch of any major initiative that requires the processing of personal data by a controller. Incorporating a DPIA as a process within your organisation can be an important step for introducing the principles of "privacy by design" and "privacy by default" to your organisation's culture.

3.5 Are there any specific processing activities which require a DPIA to be performed?

Below is a non-exhaustive list of the types of processing activities which the Commissioner considers it necessary to perform a DPIA in relation to before commencing the processing activity:

- using profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;

Example:

A mortgage broker uses automated software to decide whether or not to offer mortgages to individuals based on the area they live in, their job title and their salary.

- systematically monitoring a publicly accessible place on a large scale;
- processing special-category data on a large scale;

Example:

An insurance company collects health records of all of a large corporate customer's employees to determine the corporate customer's annual premium.

- collecting biometric data on employees for the purposes of identifying them (e.g. ror entry into a building);
- carrying out profiling (as defined in the DPR 2021) on a large scale;
- combining, comparing or matching data from multiple sources to compile a fuller picture around an individual; and
- processing personal data that could result in a risk of physical harm in the event of a security breach.

4. WHAT MUST A DPIA CONTAIN?

4.1 Generally

There is no specified format for a DPIA in the DPR 2021, however we have made available a template on our website which can be used. You can also develop your own, to suit your own organisation and requirements.

While there are minimum requirements regarding what must be considered and described in a DPIA (see next paragraph), it is not expected that a DPIA will contain absolutely every risk that may be associated with the proposed operation, process, plan or service.

However, while the DPIA does not have to eradicate all risk, it should help you minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve. By identifying the risks, you can also take steps to mitigate those risks to an acceptable level prior to commencing the processing activity. When you revisit a DPIA, you can assess how those risk mitigation tools you put in place are performing and can adjust those accordingly.

DPIAs are designed to be a flexible tool that you can apply to a wide range of sectors and projects. Conducting a DPIA does not always have to be complex and highly detailed, but there must be a level of rigour in proportion to the privacy risks arising.

4.2 What is mandated?

Section 34(5) of the DPR 2021 requires that, at a minimum, a DPIA must:

- describe the nature (i.e. how you collect, store, use, access, share personal data), scope (i.e. nature, volume, sensitivity, frequency, etc.), context (i.e. source, your relationship with data subjects, use of technology, etc.) and purpose of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals – whether physical, emotional or material. Those might include (but are not limited to);
    - bodily harm;
    - a loss of opportunity;
    - removal of access to services or product offerings;
    - processing which results in data subjects no longer being able to access certain rights which they would otherwise have (including, but not limited to, privacy rights);
    - wider access to their personal data within your organisation (or outside your organisation);
    - data which had previously been pseudonymised now being identifiable;
    - risk of impersonation or fraud; or

- social disadvantage (e.g. absence of a benefit).

- identify any additional measures to mitigate the risks identified. This could be:
  - seeking alternative technological solutions;
  - educating internal stakeholders;
  - holding personal data for shorter periods of time;
  - collecting less personal data;
  - increasing physical and IT security measures;
  - strengthening contractual terms with third party data recipients;
  - making it easier for data subjects to exercise their rights;
  - updating privacy policies;
  - updating any internal data protection guidance to account for the processing activity; or
  - processing data in non-identifiable form (e.g. anonymising personal data, where possible).

This is not an exhaustive list. You may be able to identify alternative methods to mitigate against or avoid the risks. Your Data Protection Officer (DPO) should be able to support in this regard.

4.3 What does a best practice DPIA cover?

A best practice DPIA will:

- explain why the controller needed a DPIA, detailing the types of intended processing that triggered the requirement;
- be structured clearly and be easily understandable to a reader not necessarily familiar with the processing activity. It should be written in plain English with any industry specific terminology clearly explained;
- make clear the relationships between controllers, processors, data subjects and any systems, using both text and data-flow diagrams (where appropriate). It should be clear to the reader how data is flowing between the parties and why it is flowing in that way;
- clearly state the legal bases for processing which apply in each case;
- explain how data subject rights will be supported in the context of the processing activities;
- identify all relevant risks to individuals' rights, assessed their likelihood and severity;

- explain clearly and fully how any proposed mitigation steps will reduce any identified risks;
- list any lower risk alternatives to achieving the same purpose, explaining why those were not chosen;
- detail outcomes of consultation with stakeholders (if any);
- attach any relevant documentation (e.g. consent forms, privacy notices, screenshots of portals for data collection, etc.);
- include recommendations made by the DPO; and
- document a schedule for reviewing the DPIA regularly or when the nature, scope, context or purposes of the processing changes.

5. HOW TO CONDUCT A DPIA

As per section 34(3) of the DPR 2021, the controller must seek the advice of the controller's DPO, where one is designated by that controller, when carrying out a DPIA. Advising on, and monitoring performance against, DPIAs is an explicit requirement of a DPO.

A DPIA is not just the responsibility of the DPO and / or the privacy team. It is important that the individuals or department which own the processing activity work closely with the DPO to help him or her understand how the processing operations will work (from collection through to deletion) so that the associated risks can be identified. The DPO may also involve other teams in the organisation (such as IT security teams), where those teams can support in mitigating any risks identified in the course of preparing the DPIA.

When conducting a DPIA which relates to a processing activity being undertaken in accordance with a code of conduct, the controller may refer to the code of conduct to support it in its assessment of the impact of that processing activity, as per section 38 (3)(d) of the DPR 2021.

6. WHAT IF A DPIA IDENTIFIES THAT PROCESSING IS LIKELY TO RESULT IN A HIGH RISK TO THE RIGHTS OF NATURAL PERSONS?

In the event that a DPIA identifies that the processing is likely to result in a high risk to the rights of natural persons, despite any risk mitigation measures taken by the controller, then the controller must notify the Commissioner prior to carrying out such processing (i.e. prior to the "go-live" date of the platform, portal or service which relates to the processing activity which is the subject of the DPIA). The notification must contain all the information referred to in paragraph 4.2, above.

You can notify and submit the DPIA to the Commissioner using the Registry Platform. In addition to providing feedback, the Commissioner may require corrective action to be taken prior to commencement of the processing activity which is the subject of the DPIA.

7. ONGOING OBLIGATIONS

As with the entire data protection compliance program it is important for the controller to continually monitor compliance, this includes the status of its DPIAs. The controller must carry

out a review to assess if processing is performed in accordance with the DPIA, including where there is a change of the risk represented by the processing activities.

Example:

A company conducted a DPIA because it was considering offering services to individuals under the age of 18 for the first time, meaning that it would be collecting significant amounts of personal data relating to minors, where it had not done so previously. When the DPIA was first performed the marketing team at the company were not intending on sending direct marketing emails to customers who are under 18. The rollout of the new services was not as successful as the company had hoped and, as a result, the Head of Marketing asks the DPO if it would be acceptable to collect contact details via a third party to conduct direct marketing directly to individuals under the age of 18. As the risk profile has now changed, with a new processing activity and a new source of personal data, the DPO should work with the Marketing team to update the DPIA, consider whether the new processing activity is likely to create a high risk and, if so, what mitigation measures can be put in place to reduce that risk to an acceptable level.

8. DO PROCESSORS NEED TO PERFORM DPIAS?

No. Only controllers are required to perform DPIAs under the DPR 2021. However, when being appointed by controllers, processors are required to make contractual commitments to assist controllers in ensuring compliance with certain obligations under the DPR 2021, including section 34 (DPIAs).

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.