DIFC

DATA PROTECTION IMPACT ASSESSMENTS

Commissioner of Data Protection

DIFC

CONTENTS

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

1. Introduction

The goal of the DIFC Commissioner of Data Protection (the **Commissioner**) in producing this guidance is to assist Controllers and Processors subject to the Data Protection Law, DIFC Law No. 5 of 2020 (the "DPL") and the Data Protection Regulations issued pursuant to the DPL (the "Regulations") about conducting DPIAs in accordance with Article 20.

If you require further information or clarification about anything provided in this guidance document or any other guidance referenced herein, please contact the Commissioner's Office either via the DIFC switchboard, via email at commissioner@dp.difc.ae or via regular mail sent to the DIFC main office. Also, you may wish to refer to the DIFC Online Data Protection Policy.

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

2. Scope

Due to DIFC's historical reliance on UK and EU data protection and privacy principles and the interpretation thereof by the UK authorities, from a common law perspective, this guidance has been adapted from and should be read in conjunction with existing UK guidance, as well as with EU laws and guidance on the same topic, with which the DP Law is also aligned.

*Please note that **this guidance expresses no opinion on lawfulness of specific business activities, does not have the force of law, and is not intended to constitute legal advice**. Please contact legal counsel for assistance in determining your data protection and privacy policies in respect of the issues under discussion to ensure compliance with the applicable laws and regulations. The Commissioner does not make any warranty or assume any legal liability for the accuracy or completeness of the information herein as it may apply to the particular circumstances of an individual or a firm.*

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

3. Article 20 Obligations

Article 20 of the DPL sets out when and how Data Protection Impact Assessment ("**DPIA**") should be conducted. There are many factors to consider when deciding whether to conduct a DPIA, but this decision is ultimately determined based on the likely risk to the Data Subject's rights.

This guidance aims to clarify the need for DPIAs when processing operations of a company are:

i. High Risk Processing Activities ("**HRPA**")[1] (with likely high risk to Data Subject rights) and therefore, require a DPIA before conducting such operation; and, alternatively

ii. not likely to result in high risk to Data Subject rights and, therefore, does not require prior DPIA.

Article 20(4): Types of processing operations that *DO* require a DPIA

Article 20(1) requires Controllers to conduct DPIAs before High Risk Processing Activities are undertaken. To help companies determine whether they conduct HRPA, the Commissioner's Office has produced a DP Assessment Tool, which can be found here.

At a high level, the types of processing operations that may be HRPA and therefore would ordinarily require a DPIA include:

- *Evaluation or scoring*: including profiling especially on the person's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.

- *Automated decision-making*: including where the Processing will involve a systematic and extensive evaluation of personal aspects relating to natural persons, based on automated Processing, including Profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.

[1] High Risk Processing Activities Processing of Personal Data where one (1) or more of the following applies:
(a) Processing that includes the adoption of new or different technologies or methods, which creates a materially increased risk to the security or rights of a Data Subject or renders it more difficult for a Data Subject to exercise his rights;
(b) a considerable amount of Personal Data will be Processed (including staff and contractor Personal Data) and where such Processing is likely to result in a high risk to the Data Subject, including due to the sensitivity of the Personal Data or risks relating to the security, integrity or privacy of the Personal Data;
(c) the Processing will involve a systematic and extensive evaluation of personal aspects relating to natural persons, based on automated Processing, including Profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; or
(d) a material amount of Special Categories of Personal Data is to be Processed

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

- *Sensitive Data*: a material amount of Special Categories of Personal Data (**SCPD**)[2] is being Processed including information about individuals' political opinions or criminal convictions.

- *Data processed on a large scale*: a considerable amount of Personal Data will be Processed (including staff and contractor Personal Data) and where such Processing is likely to result in a high risk to the Data Subject, including due to the sensitivity of the Personal Data or risks relating to the security, integrity or privacy of the Personal Data. When determining whether the processing is a considerable amount consider:

    - "*the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;*

    - *the volume of data and/or the range of different data items being processed;*

    - *the duration, or permanence, of the data processing activity; and*

    - *the geographical extent of the processing activity."*

- *Innovative use or applying new technological or organisational solutions which creates a materially increased risk to the security or rights of a Data Subject or renders it more difficult for a Data Subject to exercise his rights*: including combining use of fingerprint and face recognition for improved physical access control, or the development of automated / semi-automated, machine learning or large language model systems that draw from massive databases of personal data, or that create Personal Data simulating a virtual person or other persona.

This list is not exhaustive and does not absolve a Controller from responsibility for complying with DPL in all respects with regard to HRPA. For specific Processing operations that do ordinarily require a DPIA as determined by the Commissioner in accordance with Article 20(4), please review Appendix 1.

Article 20(5): Types of processing operations where a DPIA is *NOT NECESSARILY* required

Article 20(1) of the Data Protection Law also explains that a Controller may choose to carry DPIAs for other processing operations (where HRPA is not applicable). Generally, it is encouraged that Controllers conduct DPIAs to determine the risk of any processing of personal data to the data subject (even when not required under the Data Protection Law).

[2] Special Category Personal Data is Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

However, the Commissioner understands that some processing operations do not require a DPIA, i.e., where it is not likely to result in high risk to Data Subject rights, or that conducting a DPIA may be disproportionate to the type of processing undertaken or to be undertaken, or to company resources.

These instances/processing operations typically include where:

- another member of a Controller's Group has conducted a data protection impact assessment, complying with the requirements of Article 20(6), in relation to substantially the same Processing that remains current and accurate, the Controller may rely on such data protection impact assessment for the purpose of this Article 20[3];

- Processing pursuant to Articles 10(c) or 10(e) has a lawful basis in Applicable Law to which a Controller is subject, Applicable Law regulates the specific Processing operation or set of operations in question and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that lawful basis[4]; or

- the Commissioner, or another relevant, recognised regulatory authority from outside the DIFC, has acknowledged that a DPIA is not required in a specific instance and these conditions have not changed.

By way of further example, the Guidelines on Data Protection Impact Assessments (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679[5] also provide examples of where DPIA is not required:

- An online magazine uses a mailing list to send a generic daily digest to its subscribers

- An e-commerce website displays adverts for vintage car parts involving limited profiling based on items viewed or purchased on its own website.

For specific Processing operations that do not necessarily require a DPIA as determined by the Commissioner in accordance with Article 20(5), please review Appendix 2.

It is important to consider the determinations of other supervisory authorities if your company's operations span several jurisdictions. It could be for example that there is no requirement in one country to conduct a DPIA, but in another, it may be absolutely required. Taking the strictest interpretation of where such requirements exist and applying them globally to your company's operations may be application of best practice, but only you know your business well enough to decide what to do and implementing any associated policies in this regard.

[3] Article 20(2), Data Protection Law

[4] Article 20(9), Data Protection Law

[5] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (download available)

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

4. DPIA Contents, Conduct and Review

Article 20(6) addresses the content of a DPIA. The primary components include:

- a detailed description of the Processing and purposes, i.e., projects, incident management, as well as the legitimate interests of the activities;
- a necessity and proportionality assessment in relation to the purposes;
- a description of the lawful basis for the Processing under the circumstances;
- clarification of risks to Data Subjects; and
- safeguards, mitigations of risks, and security measures in place to protect the personal data and to comply with the DPL and applicable laws as well.

Article 20(10) requires that the DPIA is reviewed on a regular basis, which may even include re-doing the DPIA based on current activities, or updating it when the risks component changes.

With respect to how to conduct a DPIA, there is no set format prescribed by the Commissioner or most other supervisory authorities. There are many sensible options and approaches. Practically, it may be helpful to benchmark best practices with local regulators supervising other members of the Group, to set out the procedures that stakeholders in your business agree on, or to consult with the Commissioner's Office itself, or its assessment tools, templates and guidance.

5. Obligations of Controllers and Processors

While obligations of Controller and Processors are set out more substantively in separate guidance, Article 20 sets out a few compliance points that should be considered. There are some actions that Controllers and Processors should consider throughout the DPIA process.

DPIA Team

The DPIA should include people with sufficient expertise and knowledge of the Processing or project, such as the project team and any business owners. If your organisation does not possess sufficient expertise and experience internally, or if a particular project is likely to create a high level of risk or affect a very large number of people, it may be helpful to appoint external specialists to consult on or to carry out the DPIA.

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

Please note as well that Article 18(3)(c) requires the DPO, if one is appointed, to provide advice where requested during the DPIA process.

Transparency and Accountability

For example, Article 20(8) states that the Controller conducting the DPIA shall seek the input of Data Subjects about the intended Processing where appropriate to do so and respecting any limitations presented by protecting commercial or public interests. In a sense this means that a survey or consultation may be a useful tool for businesses to provide better, more confident outcomes of the DPIA process, both because it may flag contentious Processing activities, and otherwise demonstrates transparency and accountability to the Data Subjects and the supervisory authority. A final benefit is that if one of the associated risks of the Processing or project, etc., comes to pass, having this "consultation" in hand potentially mitigates regulatory enforcement action.

Processor Participation and Support

Finally, Article 20(11) states:

> *A Processor appointed, or in the process of being appointed, by a Controller to carry out a Processing activity shall assist the Controller by providing all information reasonably requested by the Controller in connection with the relevant data protection impact assessment.*

While in large part, conducting DPIAs seems to fall on the Controller, it is important to note that Processors have a hand in providing support to the conduct of the DPIA.

6. Questions and Comments

For further information about Article 20 DPIA requirements, please review general guidance about Obligations of Controllers and Processors, High Risk Processing & DPO Appointments, or the relevant assessment tools.

Please contact the DIFC Commissioner of Data Protection either via the DIFC switchboard, via email at commissioner@dp.difc.ae or via regular mail sent to the DIFC main office for any clarifications or questions related to this document. You may also wish to refer to the DIFC Online Data Protection Policy.

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

Appendix 1 – Processing Operations for which a DPIA is Required

Under Article 20(4), the Commissioner may at his discretion publish a non-exhaustive list of types or categories of Processing operations that are considered to be High Risk Processing Activities.

The list below is adopted from the Information Commissioner's Office of the United Kingdom (the **ICO**)[6]. Some of these operations require a DPIA automatically, and some only when they occur in combination with one of the other items.

1. **Innovative technology**: processing involving the use of innovative technologies, or the novel application of existing technologies (including AI)[7]. A DPIA is required where this processing is combined with any of the criteria from comparable, relevant guidelines.
2. **Denial of service**: Decisions about an individual's access to a product, service, opportunity or benefit that is based to any extent on automated decision-making (including profiling) or involves the processing of SCPD.
3. **Large-scale profiling:** any profiling of individuals on a large scale.
4. **Biometrics:** any processing of biometric data.
5. **Genetic data:** any processing of genetic data, other than that processed by an individual health professional for the provision of health care direct to the data subject.
6. **Data matching:** combining, comparing or matching personal data obtained from multiple sources.
7. **Invisible processing:** processing of personal data that has not been obtained directly from the data subject in circumstances where the controller considers that compliance with Article 30 of the DPL and applicable Regulations would prove impossible or involve disproportionate effort.
8. **Tracking:** processing which involves tracking an individual's geolocation or behaviour, including but not limited to employee data, or data processed in an online environment.
9. **Targeting of children or other vulnerable individuals:** the use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if the intention is to offer online services directly to children.
10. **Risk of physical harm:** where the processing is of such a nature that a personal data breach could jeopardise the (physical) health or safety of individuals.

Also, please be aware that the data protection authorities in other jurisdictions such as the EU may publish lists of the types of processing that require a DPIA in their jurisdiction.

[6] ICO Guidance on When a DPIA is Needed

[7] ICO Guidance on AI and Data Protection

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

Appendix 2 – Processing Operations for which a DPIA is Not Necessarily Required

Under Article 20(5), the Commissioner may also publish a list of the types or categories of Processing operations for which a DPIA is not necessarily required. The list below is based on the one adopted by the Commission Nationale de l'Informatique et des Libertés (the **CNIL**).[8]

1. Processing operations solely for human resources purposes by employers with fewer than 50 people, except when profiling is used

2. Processing carried out for the management of the relationship with suppliers

3. Processing carried out by an association, foundation or any other non-profit institution for the management of its members and donors in the framework of its regular activities as long as the data is not Special Category Personal Data (**SCPD**)

4. Processing of health data necessary for the care of a patient by an individual healthcare professional in a medical practice, a pharmacy or a medical biology laboratory

5. Processing carried out by lawyers in the individual practice of their profession

6. Processing carried out by DIFC Courts or other relevant commercial or civil courts for the purpose of carrying out relevant activities

7. Processing carried out by notaries for the purpose of carrying out their obligations and the drafting of notarial office documents

8. Processing carried out by government authorities, as well as legal persons covered by public and private law, for the management of schools, as well as extracurricular and early childhood services ;

9. Processing carried out solely for the purpose of managing physical access controls and schedules for calculating of working times, excluding any biometric device. The processing does not reveal sensitive data or data of a highly personal nature

10. Processing relating to breathalyser tests, implemented in the framework of transport activities, mandatory by applicable local law and restricted to the sole purpose of preventing persons from operating vehicles while under the influence of alcohol or narcotics

[8] CNIL Deliberation no 2019-118 of 12 September 2019

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.