DIFC

HIGH RISK PROCESSING ACTIVITIES AND DPO APPOINTMENTS

Commissioner of Data Protection

CONTENTS

1. Introduction

The goal of the DIFC Commissioner of Data Protection (the “Commissioner”) in producing this guidance is to assist organisations 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") to evaluate whether their data processing activities are High Risk Processing Activities and appointing a Data Protection Officer (a “DPO”), for the purposes of the DPL.

There are consequences under the DPL for Controllers and Processors that undertake High Risk Processing Activities. In order to comply with the DPL organisations must understand whether or not they carry out High Risk Processing Activities, and if so, the obligation to appoint a DPO.

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.

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 should be read in conjunction with those existing UK and 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.*

3. What are High Risk Processing Activities?

The DPL defines High Risk Processing Activity as:

> *"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."*
>
> DIFC Data Protection Law, Schedule 1, Article 3

Processing activity which satisfies one or more of the paragraphs of the definition is HRP. In order to comply with the law, Controllers and Processors will need to regularly consider whether any of their activities fall within the definition. Guidance on each paragraph is provided below, although in many cases it will be necessary for the Controller or Processor to make a judgment call and to adopt a risk-based approach. A high-level decision-tree illustrating how to determine if HRP are being undertaken is set out in Schedule 1 of this guidance.

The Commissioner would expect most well-resourced businesses, including businesses with global operations, to take a prudent approach to data protection matters. In general, such businesses would be expected to employ staff familiar with data protection issues in managerial roles. Therefore where there is a borderline Processing activity, which may or may not be a HRP, the Commissioner would expect

such staff to conduct a data protection impact assessment before proceeding. Please consider conducting the HRP assessment to determine if the entity is engaged in HRP activities.

i. 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

For this paragraph to apply, each of the following two tests must be met:

1. new or different technologies or methods are to be adopted (this could mean, for example: storing a record of transactions or other data on a blockchain rather than a traditional database; or, using artificial intelligence techniques to automate a decision making process or to gather information via "chat" features); and

2. the security or rights of the Data Subject are materially negatively impacted, or it is more difficult for a Data Subject to exercise his rights.

EXAMPLE:

A restaurant decides to introduce an electronic ordering service, where customers can log in to a mobile application and order food direct to their table without interacting with a waiter. The application requires the customer to create an account, and maintains a record of when the customer visited the restaurant and what was ordered. Previously, all ordering was done face-to-face and no personal information was captured through the ordering process. This satisfies the first branch of the test in paragraph (a).

However, the application is well designed and the restaurant has clear procedures in place to manage requests from customers to exercise their rights as Data Subjects (for example, accounts can easily be deleted, ordering history can be erased and is only stored in any event if the customer has granted permission, a copy of personal data can be provided, all necessary processing information is provided etc.). No particularly sensitive or high-risk data is being collected or used and the collected data is used only to fulfil orders more quickly.

Because there is no material negative impact on the security or rights of the Data Subject, the second branch of the test in paragraph (a) does not appear to have been satisfied and so the activity does not appear to constitute a HRP, based on that paragraph (a), even though a new Processing technology is being used.

EXAMPLE:

A motor insurance provider receives invoices from repair shops for repair works carried out on insured vehicles. The invoices are sent to a dedicated email Inbox made available by the insurance provider in .pdf format and then cross-checked against policy records, incident notifications and approvals and keyed into the provider's system by its own staff members. Each repair shop uses a different invoice format, the .pdf files are not easily machine readable and sometimes the covering email contains relevant information not contained on the invoice. As such, the process for the insurer is inefficient.

The insurance provider decides to automate the system by requiring all repair shops to submit invoices and relevant information in a single uniform format via an online portal. Submitted claims are automatically cross-checked against the insurance provider's electronic database of covered vehicles. Approved invoices are then converted into a different data format and stored on a blockchain which maintains a permanent record of the amount paid, the type of repair, the date of repair, the date and location of the relevant incident, the vehicle details and the policyholder and driver details. These activities satisfy the first branch of the test in paragraph (a) as two new and different technology and processing methods are being used.

The data on the blockchain is encrypted but a person with access to the blockchain and the policy database could be able to link repairs and the associated personal data to persons and form a picture of a person's motor incident history. In addition, other insurers are given access to a tool which can be used to interrogate the blockchain and prove whether claims stored on the blockchain relate to a particular individual or not (for the purposes of attempting to detect and managing fraudulent claims within the industry as a whole).

The blockchain cannot feasibly be edited and records cannot be removed, nor can the personal data held on it be provided in an intelligible form without great effort. However, the data capture and storage method is generally believed to be reasonably secure, and certainly more secure than the previous manual method of data entry.

Whilst there are potentially some benefits for Data Subjects, particularly around security, the new Processing method makes it harder for Data Subjects to exercise their rights to erasure, to object to Processing and to access Personal Data. Accordingly, the second branch of the test in paragraph (a) will apply and this activity will constitute HRP. The insurance provider should conduct a data protection impact assessment in relation to the activity (as well as appointing a DPO, if it does not already have one).

The Commissioner recognises that legitimate new technologies develop over time and that there is potential for tension between how such technologies are used versus their unintended effects, as well as how they impact adherence to data protection law principles and requirements. It is very hard for legislation to develop and adapt as quickly as technical innovations come to market and impact the way businesses operate. The DPL attempts to recognise the possibility of such tension and to provide some flexibility for Controllers. Articles 29(1)(h)(ix), 33(4) and 34(3) provide that by satisfying an enhanced information provision requirement, it may be possible for Controllers to lawfully refuse the exercise of certain Data Subject rights if not technically feasible. However, this specific derogation does not mean the activity is not a HRP; that question must always be considered separately.

ii. 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

For this paragraph to apply, each of the following two tests must be met:

1. a considerable amount of Personal Data will be Processed; and
2. the risk to the Data Subject is likely to be high.

The Commissioner does not want to set a specific quantitative threshold with respect to what constitutes a "considerable amount" of Personal Data but the following types of entity may typically be expected to Process a considerable amount of Personal Data:

- a Controller with several hundred staff
- a Controller with several thousand customer records
- a business which collects, stores or analyses Personal Data on behalf of its customers
- a business which collects, stores or analyses Personal Data on behalf of its Group
- a Processor which provides outsourced business services or business processes involving Personal Data, such as HR or payroll systems or processes or IT support services
- a provider of hosted subscription services or self-service online services
- a branch of an organisation which operates a shared customer loyalty scheme or other data exchange around its group
- an aggregator platform or referral platform

By contrast, the following entities may not typically be expected to Process a considerable amount of Personal Data:

- professional advisers who operate with a small client base and do not collect much Personal Data from their clients beyond named contact details (such as certain consultancy firms with a limited number of staff)
- small or medium-sized businesses with limited staff numbers that do not routinely collect customer Personal Data or only collect very limited amounts of customer Personal Data (independent retailers, galleries, food and beverage outlets, for example)
- holding companies (unless there is a considerable number of natural persons who are shareholders)

The Commissioner would like to clarify that where a merchant uses a PCI-DSS compliant card-payment solution the Commissioner does not consider that the collecting of payments via such solution will result in the Processing of a considerable amount of personal data, even if the merchant conducts a considerable number of transactions.

EXAMPLE:

A popular retailer established in the DIFC has a large customer base and has many hundreds of individual customers each day. Over the course of a year it will service thousands of customers. The retailer is an independent retailer and does not share any data with any other affiliated business.

The retailer does not ask for any Personal Data when concluding a transaction and does not maintain a customer database of any sort. It operates a loyalty scheme but this works via the customer collecting stamps on a physical card. No Personal Data is required to be provided to participate in the loyalty scheme.

The retailer rarely processes returns or complaints, due to the nature of the goods it sells.

The retailer takes numerous card payments and operates in accordance with PCI-DSS standards.

The retailer usually has between 8 and 12 staff members, including management, at any given time.

Security services (such as CCTV surveillance), cleaning services and other general business services are provided to the retailer by the local landlord and are outside the retailer's control. The retailer can only view CCTV on specific request if there is a reason to do so and does not have direct access to it.

In the Commissioner's view, this retailer is not likely to be Processing a considerable amount of Personal Data, despite having a large number of customers. If the retailer was to ask customers for an email address or mobile telephone number, or to implement its own surveillance system, then it would more likely be considered to Process a considerable amount of Personal Data.

The second paragraph of the definition requires that the risk to the Data Subjects is high, in addition to a considerable amount of Personal Data being Processed. The DPL therefore requires a risk-based approach to this question. Generally, the more limited the data set collected from each Data Subject, the lower the risk will be, unless the data itself, regardless of amount, is particularly high-risk.

Examples (non-exhaustive) of typically low-risk data include:

- name
- email address
- username
- account identifier

Examples (non-exhaustive) of typically high-risk data include:

- Special Categories of Personal Data
- bank account details, salary details or similar financial data
- copies of official documents, such as identity cards and passports
- location tracking data
- data relating to third parties gathered via the primary Data Subject

In addition to considering the data itself, the Processing activity to be carried out on the data needs to be considered to determine whether the risk to the Data Subject is high. If the retailer in the previous example collects a customer email address but only uses this for occasional direct marketing in accordance with the Legislation and other relevant laws then the risk to the Data Subject may remain low, despite the increased amount of data collection.

The assessment required is a similar assessment (considering the nature of the Personal Data and how it is to be Processed) to the assessment which needs to be made when determining the appropriate technical or organisational measures to be used, under Article 9(1)(i) of the DPL, to ensure that Personal Data is kept secure, including being protected against unauthorised or unlawful Processing (including transfers), and against accidental loss, destruction or damage. What is an appropriate technical or organisational measure will depend on the type of Processing the business undertakes and the impact and harm that might result from an unauthorised disclosure or loss of the Personal Data.

If the data collected is particularly sensitive (for example, medical data, biometric data, personal financial data) then even a very limited use of that data may create a high risk to the Data Subject. Simply storing highly sensitive data is likely to create a high risk to Data Subjects due to the risk of a data breach. As such, the Commissioner would expect virtually all medical practices and regulated financial businesses, for example, to be conducting High-Risk Processing Activities and many service providers to suppliers in those industries will also be conducting High-Risk Processing Activities (to the extent they have access to Personal Data).

iii. 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

There are three tests that must be met for this paragraph to apply:

1. a systematic and extensive evaluation of personal aspects relating to natural persons must occur; and

2. the evaluation must be automated; and

3. decisions which could have legal implications or similarly significantly affect the person must be made based on the automated evaluation.

A systematic and extensive evaluation of personal aspects relating to natural persons does not require any particular dataset or categories of Personal Data in order to occur. The Commissioner takes the view that an extensive evaluation will occur when a Controller seeks to analyse Personal Data in a way which goes beyond the immediate purpose for which it was collected in order to build a fuller picture of the natural persons concerned than would otherwise be available to the Controller, provided that such data is more than just administrative data. If the Controller is doing this as a regular part of its business-as-usual activity then the evaluation will be systematic.

EXAMPLE:

A provider of an online self-service communication platform keeps a log of when users access the platform and when they log off. When users initially create an account on the platform, the provider collects each user's name, email address, mobile telephone number, nationality and age information. The provider wishes to have its administrative account data analysed and cross-checked against user age information to increase its understanding of how long different age groups spend using the platform and what times of day different age groups prefer. The analysis will not produce any results focused on individuals and will only produce aggregated reports and insights.

In the Commissioner's view, this is unlikely to constitute a systematic and extensive evaluation of personal aspects relating to natural persons as limited insight into the profile of any natural person is likely to occur, the results are to be aggregated and the data to be analysed is largely administrative in nature.

EXAMPLE:

A provider of an online self-service communication platform keeps a log of when users access the platform and when they log off. It also keeps a log of the metadata relating to each user's communications (although it cannot see the communication content itself). When users initially create an account on the platform, the provider collects name, email address, mobile telephone number, nationality and age information.

The provider continuously conducts automated deep data analysis on all the communications metadata, including identifying where communications are personal or commercial in nature (and where they are commercial, with which business accounts), and uses it to categorise its users into various profile groups and sub-groups. It also enables profiles to be linked with user accounts in third party apps and apps offered by affiliated businesses to enable targeted advertisements and other content to be sent to its users across various platforms, based on an algorithm which uses the profiling data already created.

In the Commissioner's view, this is likely to constitute a systematic and extensive evaluation of personal aspects relating to natural persons as the insights gathered go beyond those necessary to understand and optimise the provider's own service offering, are deliberately intended to build a broader picture of users and will be used in ways outside the primary purpose of the communication platform.

Whether or not the evaluation is automated should be a question of fact and detailed guidance is not required.

The final aspect of the test is that decisions which could have legal implications or similarly significantly affect the person must be made based on the automated evaluation. If the evaluation profile of the person will be used to decide whether to offer, for example (non-exhaustive):

- an employment contract
- a real estate lease
- a personal loan
- an insurance contract

or on what terms to offer the above, then there is likely to be a significant impact on the person concerned and a potential legal impact.

If the profile is to be used in a disciplinary context, or a competitive context (such as determining a workplace promotion), then it is likely to have a significant impact on the person concerned.

If the profile is to be used to influence the communications made available to the person concerned (such as targeted political adverts) then it may also have a significant effect on the person.

The above examples are non-exhaustive.

iv. A material amount of Special Categories of Personal Data is to be Processed

Any entity which regularly Processes a material amount of Special Categories of Personal Data is engaged in HRP.

Controllers may process Special Categories of Personal Data in relation to staff (in connection with health conditions, sickness absences, disability adjustments etc) but unless the Controller has a large number of staff this activity alone may not constitute Processing of a material amount of Special Categories of Personal Data. Where Controllers do have a large number of staff and Process Special Categories of Personal Data in relation to such staff then this paragraph is likely to apply.

The Commissioner views this paragraph of the definition as being targeted more at Controllers which, by virtue of the nature of their business, Process material amounts of Special Categories of Personal Data. Such Controllers may include (non-exhaustive) medical or general health and wellbeing related businesses, research businesses, profiling and analysis businesses, security and surveillance businesses, investigatory businesses, regulatory bodies and public authorities. The question of materiality is linked to the sensitivity of the Personal Data in question; the more sensitive the data and the more potential there is for the Data Subject to suffer harm as a result of the misuse or loss of the data, the lower the volume of data needs to be for the amount of data to be material.

4. What are the consequences of performing High Risk Processing Activities? Must I appoint a DPO?

This section sets out the direct consequences that arise if an entity conducts HRP, in addition to consequences that may also arise from the Processing in question. For example, there may be a requirement to consult with the Commissioner under Article 21 but this will not occur in all cases.

Regardless of whether the Processing in question is a HRP or not, the general requirements of the DPL relating to Processing will always apply, including Part 2 (General Requirements).

i. Data Protection Officer

Any Controller or Processor subject to the DPL that performs HRP on a systematic or regular basis must appoint a DPO.[1] Please consider using the DPO appointment assessment tool available on the Guidance page of the DIFC DP website.

The Commissioner considers that an entity performing HRP should be able to demonstrate a mature and comprehensive level of internal compliance with the Legislation and that it is appropriate for such entities to have a DPO with knowledge of the Legislation to monitor the entity's compliance.

The required competencies and status of a DPO are set out in Article 17 of the DPL. The role and tasks of a DPO are set out in Article 18 of the DPL. The DPO is also responsible for overseeing data protection impact assessments under Article 20 of the DPL.

Article 16 of the DPL provides flexibility to entities with respect to the terms of engagement of the DPO (staff, Group company staff or independent contractor). Groups of entities may have a single DPO. Additionally, where the entity subject to the DPL is part of an international Group the DPO may be based outside the UAE if the DPO performs a similar role for the Group on an international basis. Ideally, the DPO should be an individual. If there is a request by an entity to appoint an organisation as a DPO for specific, valid reasons, please contact the Commissioner's Office for consultation.

[1] In addition, DIFC Bodies other than Courts acting in their judicial capacity must appoint a DPO (Art. 16(2)(a). Any Controller or Processor may also elect to appoint a DPO (Art. 16(1)).

ii. Annual assessment for Controllers

Any Controller required to appoint a DPO (which necessarily includes Controllers conducting HRP) must carry out an annual assessment of its Processing activities, pursuant to Article 19 of the DPL.

The annual assessment must indicate whether HRP are likely to be performed during the following annual period.

Guidance on completing the DPO annual assessment is available on the DIFC DP website.

iii. Data protection impact assessment

Before a Controller undertakes any HRP it must carry out an impact assessment of the proposed Processing operations on the protection of Personal Data, considering the risks to the rights of the Data Subjects concerned, pursuant to Article 20 of the DPL.

A single impact assessment may address a set of similar Processing operations that present similar risks. If another member of a Controller's Group has conducted a data protection impact assessment that complies with the requirements of the Legislation 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 Article 20.

The Commissioner considers that data protection impact assessments do not need to be repeated every time HRP is to occur, where such activity, in terms of the nature and means of the Processing, the type of data to be Processed and the categories of Data Subjects affected, has already been assessed. For example, where a Controller conducts a HRP with respect to a particular database and gathers a number of new Data Subject records to add to the database, it is not necessary for the Processing activity with respect to the database to be reassessed if it is a non-material increase in volume of data. It will, however, be necessary for the Controller to ensure that the Processing is lawful and compliant with the Legislation with respect to the new data records and Data Subjects, including that such new Data Subjects were provided with sufficient information in relation to the Processing in accordance with the Legislation and that such Processing has a lawful basis.

5. Questions and Comments

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.

Schedule 1: Decision Checklist for High Risk Processing Activity

1.a Are we adopting a new or different technology or method of Processing?

No

Yes

1.b Does the new technology or method create a materially increased risk to the security or rights of a Data Subject or render it more difficult for a Data Subject to exercise his rights?

No

Yes

High Risk Processing Activity

2.a Will a considerable amount of Personal Data be Processed?

No

Yes

2.b Is such Processing likely to result in a high risk to the Data Subject?

No

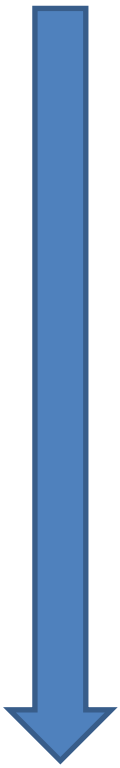
Yes

High Risk Processing Activity

3.a Will the Processing will involve a systematic and extensive evaluation of personal aspects relating to natural persons?

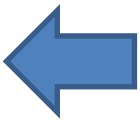
No

Yes



3.b Is the Processing automated?

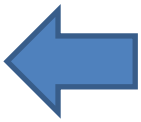
No



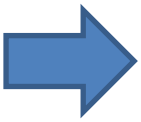
Yes

3.c Will the Processing influence decisions which could have legal implications or similarly significantly affect the person?

No



Yes



High Risk Processing Activity

4. Will a material amount of Special Categories of Personal Data be Processed?

No

Not High Risk Processing Activity

Yes

High Risk Processing Activity

Schedule 2: Examples of High Risk Processing Activities

Article 20(4) of the DPL provides that the Commissioner may at his discretion publish a non-exhaustive list of types or categories of Processing operations that are considered to be HRP. Such a list is not intended to be exhaustive and does not absolve a Controller from responsibility for complying with the DPL in all respects with regard to HRP.

Pursuant to Article 20(4), and subject always to careful application of the relevant tests, the Commissioner believes that the following types or categories of Processing operations may generally be assumed to be HRP. The likely relevant paragraphs of the definition in the DPL are indicated and types of business which may conduct the activity in question are also indicated. This list is non-exhaustive and non-binding.

The list does not consider paragraph (a) of the definition because it is to a large extent independent of the activity involved and will be assessed based on new and emerging methods from time to time.

Activity	Relevant paragraphs of definition	Examples
Processing of medical information (other than on an incidental basis such as in an employment context for example, where the amount may not be considerable or material)	(b) and (d)	- medical practices - wellness centres - fitness centres - medical regulators and supervisory authorities - hosting and data storage service providers - insurance providers - insurance brokers - claims administrators
Processing considerable amounts of personal financial data, other than collecting card payments through secure PCI-DSS compliance solutions	(b)	- banks - savings and investments providers - credit providers - employers with large payrolls

Activity	Relevant paragraphs of definition	Examples
Processing large databases containing information which could be used to harm the Data Subjects	(b) and potentially (d)	- any business with a large customer database containing data beyond basic contact data - any business with a large number of employees - any business processing a large amount of client data - any commercial-scale provider of hosted services - any information storage service - any public body or authority processing large amounts of Personal Data
Processing considerable amounts of data relating to third party natural persons who are not involved in the data collection process	(b)	- organisations which collect material volumes of data relating to dependents or associates of primary contacts - providers of electronic apps or platforms which harvest data of third parties - data aggregators - investigatory, surveillance and security organisations
Providing outsourced business process services using Personal Data that could be used to harm the Data Subjects	(b) and potentially (c) and (a)	- business process outsourcing providers - outsourced service providers - IT support service providers
Participating in data flows between companies involving large volumes of Personal Data	(b)	- multinational businesses - vertically integrated businesses - data aggregators
Processing data for the purposes of profiling a natural person and making decisions based on the profiling	(c)	- marketing businesses - data analytics businesses - artificial intelligence developers and providers - surveillance businesses - consultancies providing data analysis services - data scraping businesses
Carrying out investigatory functions	(b) and potentially (c) and (d)	- responsible authorities and bodies