DIFC DATA PROTECTION POLICY GUIDANCE
Commissioner of Data Protection

FINES AND OTHER SANCTIONS

Contents

1. Introduction

The goal of the DIFC Commissioner of Data Protection (the "Commissioner") in producing this guidance is to inform organisations subject to the DIFC Data Protection Law, Law No. 5 of 2020 (the "DPL") and the Data Protection Regulations issued pursuant to the DPL (the "Regulations") about the potential consequences of violating the DPL.

The consequences include: administrative fines; general fines; compensation claims; adverse publicity.

2. Scope

The guidance is issued by the Commissioner pursuant to Article 46(3)(h)(iii) of the DPL. In accordance with Schedule 1, Section 2(g) of the DPL, guidance issued under the DPL is indicative and non-binding.

This guidance is based on the DPL and the Regulations (collectively, "Legislation") as at 1 July, 2020 and remains current unless and until updated, withdrawn or replaced. Please visit www.difc.ae to read the full text of the Legislation.

This guidance comprises the Commissioner's interpretation of the Legislation and is issued in furtherance of the Commissioner's obligation to pursue the objectives of promoting observance of the Legislation and promoting greater awareness and public understanding of data protection and the requirements of the Legislation in the DIFC, pursuant to Article 46(2) of the DPL.

If a capitalised term is used in this guidance then it has the meaning given to it in the Legislation unless another meaning is specified.

This guidance may be updated from time to time. Readers are advised to check the DIFC website or contact the Commissioner's office for updates.

Please note that this guidance does not have the force of law and it is not intended to constitute legal advice; you should not rely on it as such. 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.

3. Commissioner's Powers

The Commissioner's objectives are defined under Article 46(2) of the DPL as follows:

(a) to monitor, ensure and enforce compliance of the DPL;

(b) to promote good practices and observance of the requirements of the DPL and the Regulations by a Controller or Processor; and

(c) to promote greater awareness and public understanding of data protection and the requirements of the DPL and the Regulations in the DIFC.

The Commissioner has a range of powers available under the law which it can use in furtherance of its objectives. Relevant powers in connection with the enforcement of the DPL are set out below.

Ability to audit Controllers and Processors	Article 46(3)(a)
Ability to conduct investigations and inspections	Article 46(3)(b)
Ability to issue directions requiring a Controller or Processor to do or refrain from doing anything (including Processing specified Personal Data)	Article 46(3)(c) and Article 59
Ability to issue warnings or admonishments	Article 46(3)(c)
Ability to make recommendations to a Controller or Processor, including ordering the appointment of a data protection officer	Article 46(3)(c)
Ability to initiate court proceedings for contraventions of the law	Article 46(3)(d)
Ability to impose fines for non-compliance with a direction	Article 46(3)(e)[1] and Article 62
Ability to impose fines for non-compliance with the Law and any Regulations and the ability to set corresponding limits on or schedules of such fines	Article 46(3)(f) and Article 62
Ability to initiate compensation claims on behalf of Data Subjects where there has been a material contravention of the DPL	Article 46(3)(g)
Ability to prepare Regulations, standards or codes of practice and guidance	Article 46(3)(h) and (i)
Ability to request provision of information from Controllers and Processors	Article 52
Duty to receive and consider complaints lodged by Data Subjects	Article 60

Policy approach and rationale for fines

The Commissioner of Data Protection recognises that many businesses handle large volumes of data constantly and that in some cases it is hard for Controllers to define in advance exactly what Personal Data they will receive from Data Subjects (for example, where there is a free text box on an online form).

The Commissioner of Data Protection also recognises that compliance is a function of various independent factors including: written procedures and processes; technical and operational measures; awareness and

[1] Fines for this contravention are not subject to a maximum limit under Schedule 1 of the DPL.

training; individual integrity and diligence. It is possible for an organisation to begin a day's business with a sophisticated set of up-to-date procedures and policies; high-grade information technology security measures and a skilled and well-trained workforce but to end the day with a significant data breach as a result of a momentary lapse of judgment by a staff member or the actions of a malicious third party.

In addition, it is recognised that the DPL does require work, preparation and investment of resource if an organisation is to satisfy itself that it has complied with the various provisions.

The Commissioner of Data Protection has developed a set of maximum fine levels for administrative breaches of the DPL to provide boundaries for the financial risks associated with such breaches. The upper fine levels are designed to create reasonable incentives for compliance, without being punitive; it is also important to note that the Commissioner will take into account the resources of an infringing company and the risk-profile of its Processing activities when assessing whether or not the maximum fine is appropriate or whether a lower fine is appropriate in the circumstances.

The Commissioner wants to encourage an environment of openness in relation to Personal Data issues within the DIFC and does not believe that imposing onerous fines on businesses for relatively minor administrative breaches of the DPL is likely to encourage such an environment.

The maximum levels of administrative fine, determined by reference to the provision of the DPL that is violated range from USD 10,000 to USD 100,000. It should be noted that the highest maximums relate to violations of provisions governing Data Subject rights; in other words, where the impact on the individual Data Subject of violation is potentially most direct. The lower maximums relate to the more administrative aspects of the DPL and to the assessment of requests for Personal Data from official authority (it being recognised that Controllers can be placed in unenviable positions of conflicting legal obligation where extra-territorial official requests are received).

The imposition of a general fine is likely to be an exceptional occurrence and the Commissioner of Data Protection hopes it is rarely necessary for it to do so. Please refer to section 7 for information on the rationale for issuing general fines.

Each violation that is investigated by the Commissioner will be assessed on its own merits, taking into account all circumstances, including previous violations, the status and activities of the offending party and the risk of harm to Data Subjects. The purpose of the Processing will also be assessed to consider the extent to which the Processing upholds the principle of purpose specification and compatible use. The duration of a violation is also an important factor because it may be illustrative of: (a) wilful conduct on the offender’s part; (b) failure to take appropriate preventive measures or to have in place processes to identify and report breaches; (c) failure to take action to mitigate the breach; and/or (d) inability to put in place the required technical and organisational measures.

Evidence that the violation is intentional in nature will naturally tend towards greater use of enforcement powers and fines, compared with unintentional infringements.

The degree to which the offending party cooperates with the Commissioner's investigation will also be a relevant factor.

Where the Controller or Processor has adhered to an approved code of conduct or a certification scheme (under Articles 48 and 50, respectively), the Commissioner may be satisfied that the body in charge of administering the code or certification scheme takes the appropriate action themselves against their member, for example through the monitoring and enforcement schemes of the code or certification scheme. If such measures are considered effective, proportionate or dissuasive enough in that particular case without the need for imposing additional measures then the Commissioner may decide that no further action is needed. The powers of the Commissioner, however, are independent of the powers of the body supervising the code or certification scheme and the Commissioner is not under an obligation to take into account sanctions imposed under the code or regulatory scheme.

4. Supervision and accountability

Administrative accountability

Part 2 of the DPL sets out various general requirements in relation to the Processing of Personal Data. In particular, Controllers and Processors have a number of requirements to comply with (predominantly in Part 2D of the DPL), which enable the Commissioner of Data Protection to carry out its supervisory function in an orderly and transparent manner.

An overarching requirement for Controllers and Processors is the requirement to establish a compliance programme and to be able to demonstrate that such programme exists and is being implemented (Article 14(1)) and to register with the Commissioner of Data Protection (Article 14(7)). If a violation brings a business to the attention of the Commissioner of Data Protection then an inability to demonstrate that a compliance programme has been developed and is in implementation is likely to be an aggravating factor, as will a failure to have notified. On the other hand, if the business can demonstrate a good attempt to develop and implement a compliance programme but has suffered a "slip up" then this may be a mitigating factor.

Similarly, Controllers are required to maintain records of Processing activities under Article 15. The inability to produce any records is likely to be interpreted as indicative of a disregard for the DPL.

Organisational accountability and supervision

If an organisation is required to appoint a DPO then the Commissioner would expect the DPO to be able to produce evidence of the organisation's compliance activities. If an organisation has voluntarily appointed a DPO then this may help to establish the organisation's commitment to compliance with the DPL (provided the DPO has been given the necessary support to fulfil his or her role).

The DPL provides for data protection impact assessments to be carried out in certain circumstances (Article 20). If a Controller does not conduct an assessment when they should have done, or conducts an assessment which is superficial or incomplete, this will likely be an aggravating factor with respect to any violation occurring due to the Processing which should have been assessed. If an assessment identifies material risks associated with Processing then the Controller will be expected to be able to demonstrate that reasonable measures to mitigate such risks have been considered and, if appropriate, implemented. If a violation would have been prevented by the imposition of reasonable measures which have, or should have been, identified then this is likely to be considered an aggravating factor.

The Commissioner may see evidence of good data protection risk assessment, even if not compulsory under the DPL, as mitigating evidence in relation to violations which later occur in relation to the Processing in question.

The DPL also includes a mechanism for prior consultation with the Commissioner in Article 21. This is mandatory in the circumstances set out in Article 21(1) but can be done voluntarily under Article 21(3). Prior consultation with the Commissioner may be viewed as a mitigating action if a violation subsequently relates to the Processing in question (unless the outcome of the consultation has been ignored or wrongly implemented).

Technical and organisational information security measures

Under Article 14(2)(b), Controllers and Processors must implement appropriate technical and organisational measures which ensure a level of security appropriate to the risks associated with the Processing and to protect against unlawful forms of Processing. Such measures should be reviewed periodically to reflect legal, technical and operational developments.

The Commissioner recognises that there is no single "right" approach to technical and organisational information security. In the same way that appropriate security for a 20 Dollar note differs from appropriate security for a country's sovereign gold reserves, what is appropriate for a Controller or Processor, with respect to information security, will be influenced by the activities and resources available to such businesses.

The Commissioner would generally expect well-resourced businesses processing large volumes of Personal Data, or undertaking High Risk Processing Activities, to make use of best-in-class, international-standard information security specialists (either as employees or third party consultants of contractors) and to be able to

demonstrate adherence to recognised international standards. This may include maintaining an information asset inventory, deploying up-to-date and well maintained hardware and software, including sophisticated firewalls and other anti-intrusion measures, configured as necessary to reflect the organisation's activities and risk-profile. Such businesses should have clear and comprehensive policies to govern organisational security, including how devices are accessed and used and how information is to be handled and stored (and how long for).

By contrast, a smaller business conducting low-risk Processing may be implementing appropriate technical security measures by largely relying on off-the-shelf third-party offerings and basic technical support, without the need for further expert assistance.

5. Directions (Article 59)

The Commissioner may issue a direction to a Controller or Processor if the Commissioner is satisfied that the party in question has contravened, or is contravening, the DPL.

The direction may require the party in receipt to do or refrain from doing any act or thing within a specified period or to refrain from Processing any Personal Data as specified in the direction, including for any particular purpose or in any manner.

A direction may be issued before any fine is issued with respect to the contravention in question and compliance with the direction may result in no further action being taken. However, the Commissioner is not obliged to issue a direction in lieu of any other sanction and may issue a direction as well as taking any other action within its powers. The issuing of, and compliance with, any direction does not prejudice the right of Data Subjects to seek compensation in the Courts or the ability of the Commissioner to impose fines.

The failure to comply with a direction is itself a contravention of the DPL and may lead to the imposition of a fine in accordance with Article 46(3)(e). In addition, the Commissioner may apply to the Court for further orders to be made with respect to the non-compliance. At the time of writing this guidance, a fine issued under Article 46(3)(e) is a general fine and is not subject to the caps on administrative fines set out in Schedule 2 of the DPL.

6. Administrative Fines (Article 62(2))

Schedule 2 of the DPL sets out a range of contraventions and associated maximum administrative fines.

The largest maximum administrative fines relate to contraventions of the provisions of Part 6 of the DPL, which relate to the rights of Data Subjects. This is reflective of the guiding principle behind the DPL, which is the protection of individuals.

Administrative fines are intended to be dissuasive and proportionate with respect to breaches of the DPL. Nevertheless, the Commissioner retains wide discretion to issue general fines under Article 62(3) and is not constrained by the amounts set out in Schedule 2 of the DPL for violations of a more serious nature (see section 5 below).

Under Article 62(4), if an administrative fine is issued then payment of the fine will ensure that the Commissioner does not commence any further proceedings against the Controller or Processor, unless a violation is ongoing.

If an administrative fine is issued but not paid within the required timescale (provided an objection is not ongoing) then the Commissioner may apply to the Court for further Court orders to enforce the fine and recover costs.

The issue or settlement of an administrative fine does not stop any separate claim that a Data Subject may have for compensation with respect to the violation in question.

7. General Fines (Article 62(3))

The Commissioner retains wide discretion to issue general fines under Article 62(3) of the DPL. Such fines are not subject to any prescribed maximum level.

General fines are intended to be issued when the violation in question is of a more serious nature than a purely administrative nature.

Factors which may be considered serious and which could lead to the imposition of a general fine include (without limitation):

- knowingly breaching the DPL
- disregard for the DPL, in particular where the Controller or Processor is not able to demonstrate any meaningful steps towards compliance or the steps taken are not commensurate with the resources and profile of the Controller or Processor
- unlawful use of Personal Data in a way which could cause material harm to the Data Subjects
- unlawful sharing of Personal Data for commercial purposes
- taking steps to conceal the use of Personal Data without lawful grounds for doing so
- failure to cooperate with the Commissioner
- repeat violations which indicate a failure to address previous non-compliance

Under Article 62(4), if a general fine is issued then payment of the fine will ensure that the Commissioner does not commence any further proceedings against the Controller or Processor, unless a violation is ongoing.

If a general fine is issued but not paid within the required timescale (provided an objection is not ongoing) then the Commissioner may apply to the Court for further Court orders to enforce the fine and recover costs.

The issue or settlement of a general fine does not stop any separate claim that a Data Subject may have for compensation with respect to the violation in question.

Factors which may be taken into account by the Commissioner when determining the level of a general fine include:

- the turnover of the violating entity
- the nature, gravity and duration of the infringement
- whether the infringement was intentional or negligent
- whether actions were taken to mitigate the damage
- whether the breach reporting requirements in the DPL were complied with
- relevant previous violations

8. Objections and appeals to the Court

Review of direction

Under Article 59(7), any party in receipt of a direction may, within 14 days of receipt, ask the Commissioner to review the direction.

Objection to a fine under DPL process

Under Article 62(6) Controllers and Processors have the right to object to a fine (whether administrative or general). The DIFCA Board of Directors shall make further Regulations to define the objection process.

Legal right to appeal to the Courts

In addition to the DIFCA objection process, Controllers or Processors may appeal to the Court under Article 63 in relation to any finding of contravention of the DPL. There is a thirty-day time limit within which to register an appeal.

9. Public reprimands

Under Article 59(9) the Commissioner may issue a public reprimand to a Controller or Processor that has infringed the DPL. A public reprimand has the potential to cause material adverse damage to the public image of a Controller or Processor and the Commissioner will not typically issue a public reprimand without first having served a direction and permitted the violating party reasonable time to remedy the violation. The Commissioner, however, is not obliged to do so. For various reasons, including if there is a particularly serious violation of the DPL and to dissuade further violations (by the offending party or other parties), the Commissioner may wish to issue a public reprimand.

10. Compensation (Article 64)

Data Subject claims

A Data Subject who suffers material or non-material damage by reason of any contravention of the DPL or the Regulations may apply to the Court for compensation from the Controller or Processor in question. The award of any compensation by the Courts is separate and independent from any fines issued by the Commissioner under the DPL.

Articles 64(2) and (3) contain provisions to allocate the risk of compensation between Controllers and Processors. Controllers will always be liable for damage caused by Processing under their control. Where a Processor is involved in the Processing, the Processor will only have liability where it has not complied with the obligations of the DPL directed at Processors or where it has acted outside or contrary to the lawful instructions of the Controller (in other words, where it has itself violated the DPL or acted outside the proper role of a Processor).

To the extent more than one party is liable for compensation in relation to Processing, Article 64(3) provides for joint and several liability in order to ensure effective compensation of the Data Subject. It will therefore be good practice for Controllers and Processors to clearly address liability issues in their contracts.

Parties are free to reach a legally binding settlement of any compensation claim outside court (by mutual agreement).

Commissioner instigation of claims

Under Article 62(8) the Commissioner may request the Court to make an order for damages or compensation payable to a Data Subject, even if he has not made a claim in accordance with Article 64. The principles in Article 64 will be considered when making the request to the Court. The Commissioner shall not make such requests unless in his opinion the Data Subject in question has suffered material damage as a result of the breach in question and is disadvantaged in his ability to bring a claim to the Court in his own name (for example, due to lack of resource or geographical remoteness or because the facts of the claim are highly complex and may not be available to the Data Subject).