CONSULTATION PAPER NO. 6

June 2019

PROPOSED NEW DATA PROTECTION LAW

CONSULTATION PAPER NO. 6
PROPOSALS RELATING TO A NEW DATA PROTECTION LAW

Why are we issuing this paper?

1. This Consultation Paper No. 6 of 2019 ("Consultation Paper") seeks public comments on the proposal by the Dubai International Financial Centre Authority (**DIFCA**) to issue legislation on the protection of personal data through a new Data Protection Law (the **Proposed Law**).

Who should read this paper?

2. This Consultation Paper would be of interest to: persons conducting or proposing to conduct business in the DIFC who will Process Personal Data as part of their business; persons who deal with such persons; and persons whose Personal Data is Processed by such persons. In particular:

   (a) companies currently operating in the DIFC or intending to operate in the DIFC;

   (b) employees and customers of such companies;

   (c) parties seeking to enter into transactions with companies in the DIFC, including by providing services to companies in the DIFC;

   (d) international groups of companies with data-flows in and out of the DIFC;

   (e) legal advisors and compliance advisors.

How to provide comments

3. All comments should be provided to the person specified below:

   Jacques Visser
   Chief Legal Officer
   DIFC Authority
   Level 14, The Gate, P. O. Box 74777
   Dubai, United Arab Emirates
   or e-mailed to: consultation@difc.ae

4. You may choose to identify the organisation you represent in your comments, if applicable.

5. DIFCA reserves the right to publish, on its website or elsewhere, any comments you provide, unless you expressly request otherwise at the time the comments are made. Comments will be published anonymously.

What happens next?

6. The deadline for providing comments on the proposals in this Consultation Paper is August 18, 2019.

7. Once we receive your comments, we will consider if any further refinements are required to the Proposed Law. Once DIFCA considers the Proposed Law to be in a suitable form, it will be enacted as a new DIFC law to come in to force on a date specified and published.

8. The Proposed Law is in draft form only. You should not act on it until the Proposed Law is formally enacted. We will issue a notice on our website when this happens.

Defined terms

9. Defined terms are identified throughout this paper by the capitalisation of the initial letter of a word or of each word in a phrase and are defined in the Proposed Law or in this paper. Unless the context otherwise requires, where capitalisation of the initial letter is not used, the expression has its natural meaning.

Background

10. Companies increasingly generate, store and use large amounts of Personal Data. Advances in technology and computing power have broadened the use-cases for such Personal Data. It is recognised across the international legislative landscape that the collection and use of Personal Data requires regulation in order to protect the rights and freedoms of individuals and to provide transparency and accountability.

11. The DIFC passed Data Protection Law DIFC Law No.1 of 2007 (**Current Data Law**) 12 years ago. The Current Data Law was amended by Data Protection Law Amendment Law, DIFC Law No.5 of 2012 and by DIFC Laws Amendment Law, DIFC Law No. 1 of 2018.

12. The Current Data Law is based on concepts deriving from the European Data Protection Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data). The Data Protection Directive was superseded in May 2018 by the General Data Protection Regulation (Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (**GDPR**), repealing Directive 95/46/EC (Data Protection Directive)).

13. Laws like GDPR have a broad impact on the international business landscape. The amount of jurisdictions, globally, enacting data protection laws is increasing and the

concepts enshrined in EU data protection law, arguably the most influential of these laws, are turning up in many other jurisdictions.

14. Throughout the Middle East, there are an increasing number of laws being passed which are concerned with data protection.

15. Given the above, the DIFC asserts that:

(a) increasing amounts of Personal Data are likely to be collected by businesses in the DIFC;

(b) the ways in which such Personal Data are used are likely to evolve, creating new risks for individuals and presenting new challenges for business;

(c) some businesses in the DIFC will be directly affected by the GDPR (and potentially by other international data protection laws);

(d) many businesses within the DIFC operate on an international scale or within an international business landscape where expectations in relation to data protection are evolving; and

(e) the foundation upon which the Current Data Law is based has been superseded.

16. To provide consistency and familiarity for businesses within the DIFC, DIFC proposes to replace the Current Data Law (and the Regulations made under it) with the Proposed Law. The Proposed Law is based on principles and concepts found within the GDPR together with modifications reflecting latest technology, privacy and security law developments as well as the unique requirements of the DIFC. The purpose of the revisions made in the Proposed Law is to ensure continuity (with respect to the Current Data Law), consistency (with respect to the broader international landscape) and to reflect modern data management thought leadership.

Key features of the Proposed Law

17. The key features of the Proposed Law include the following:

(a) setting out the principles for the Processing of Personal Data and the lawful bases which may be relied upon to Process Personal Data and Special Categories of Personal Data;

(b) making Processors directly responsible under the law with respect to certain obligations;

(c) compliance obligations including record keeping, designation of a data protection officer and carrying out data protection impact assessments (where required);

(d) obligations relating to the relationships between Joint Controllers and between Controllers and Processors;

(e) revised provisions relating to the transfer of Personal Data outside the DIFC, including controls on transfers of Personal Data to jurisdictions which do not provide an adequate level of protection for Personal Data;

(f) provisions governing responses to requests for sharing of Personal Data with governmental authorities, competent authorities, enforcement agencies etc.;

(g) provisions prescribing the information which must be provided to Data Subjects;

(h) provisions granting rights to Data Subjects (withdrawal of consent, access, rectification, erasure, right to object, portability, right not to be subject to a decision based solely on automated Processing);

(i) introduction of the principle of non-discrimination;

(j) breach notification requirements;

(k) maintaining the Commissioner of Data Protection's role in administering the data protection law in the DIFC, exercising powers and functions and participating in consultation with Controllers;

(l) provisions for approved codes of conduct and certification schemes and bodies; and

(m) provision for exemption of certain DIFC bodies on a case-by-case basis, provided conditions are met and processes are followed to enable the Commissioner of Data Protection to assess the requested exemption.

Relevant UAE laws

18. The UAE Penal Code applies in the DIFC and provisions of the Penal Code which relate to the invasion of privacy or the misuse of personal information remain relevant.

19. Federal Law No. 5 of 2012 on Combatting Cybercrimes applies in the DIFC and the provisions of the law which deal with the use of personal information online remain relevant.

20. Federal Law No. 2 of 2019 which governs the use of IT systems in the healthcare sector applies in the DIFC and contains provisions governing personal data.

21. Dubai Law No. 26 of 2015 Regulating Data Dissemination and Exchange in the Emirate of Dubai applies to persons who produce, own, disseminate or exchange data relating to the Emirate of Dubai and who are prescribed by Dubai Data Establishment (including entities in the DIFC). It includes provision requiring the protection of personal data and sensitive personal data.

22. The Proposed Law will not generally exempt any person to whom relevant provisions of the Dubai Financial Services Authority-administered legislation applies from requirements applicable to that person under such legislation. Certain limited exceptions may apply.

Application of the Proposed Law (Article 5)

23. The Proposed Law applies in the DIFC. The Proposed Law applies to the Processing of Personal Data in the context of the activities of a Controller or a Processor operating, conducting or attempting to conduct business in or from the DIFC, regardless of whether the Processing takes place in the DIFC or not. This scope ("operating, conducting or attempting to conduct business in or from the DIFC") is consistent with other DIFC law (see, for example the Operating Law, DIFC Law No. 7 of 2018, at Article 3(2): https://www.difc.ae/files/6215/4505/5154/Operating_Law_DIFC_Law_No._7_of_2018.pdf). The clarification that the actual location of Processing is immaterial has been introduced to avoid any doubt that may otherwise have existed with respect to DIFC businesses which carry on their Processing activities outside the DIFC.

24. The Proposed Law applies to the Processing of Personal Data:

(a) by automated means; and

(b) other than by automated means where the Personal Data form part of a Filing System or are intended to form part of a Filing System.

Q1. If you believe the scope of the law is unclear then please provide comments as to why.

Requirements for legitimate and lawful Processing (Articles 9 - 13)

25. Article 9 of the Proposed Law sets out general requirements for the Processing of Personal Data which reflect common data protection principles.

26. Article 10 sets out the lawful bases for Processing Personal Data and Article 11 sets out the bases under which Special Categories of Personal Data may be Processed.

27. In the Current Data Law, it was possible to rely on the following basis to Process Special Categories of Personal Data:

> "*[Special Categories of Personal Data shall not be Processed unless] necessary to uphold the legitimate interests of the Controller recognised in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by compelling legitimate interests of the Data Subject*".

The Proposed Law does not contain this basis, either in relation to Special Categories of Personal Data, or Personal Data in general terms. It is felt that the other bases set out in the Proposed Law would deem this basis redundant.[1]

28. The ability to process Special Categories of Personal Data to comply with audit and accounting requirements has been removed on the basis that such requirements could typically be satisfied without using Special Categories of Personal Data; however, if there is a specific legal obligation which requires Special Categories of Personal Data to be Processed then Article 11(1)(g) is available.

29. The concept, contained in the Current Data Law, of the Commissioner of Data Protection issuing a permit for the Processing of Special Categories of Personal Data has been omitted. The bases set out in Article 10 and 11 define when Special Categories of Personal Data can be Processed and the Commissioner does not believe there is any benefit in retaining the permit concept.

30. Article 12 provides information in relation to the use of Data Subject consent as a basis for Processing. Controllers should carefully consider the requirements in relation to obtaining valid consent, be mindful of a Data Subject's right to withdraw consent, and note that consent cannot be assumed to last indefinitely (in the absence of its withdrawal).

31. Article 13 provides guidance on reliance on legitimate interests as a basis for Processing Personal Data. As justification for carrying out activities required to perform public functions, public authorities shall not rely on this basis.

Q2. With reference to section 7, do you believe the omission of: "*[Special Categories of Personal Data shall not be Processed unless] necessary to uphold the legitimate interests of the Controller recognised in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by compelling legitimate interests of the Data Subject*", will prove problematic? If you are a Controller, what activities do you perform in reliance on this basis that could not be performed in reliance on one of the other bases?

[1] See, for example, the legitimate interests basis at Article 10(1)(f) and the compliance with Applicable Law basis at Article 10(1)(c)).

Q3. With reference to section 28, please advise if you believe you have audit and accounting requirements which require the Processing of Special Categories of Personal Data and which are not mandatory legal requirements.

Q4. Please let us know if you have any concerns or comments in relation to the conditions for reliance on consent as a basis for Processing, in particular in relation to Article 12. Please note that the ability of a Data Subject to withdraw consent will not be compromised.

Q5. Please let us know if you have any concerns or comments in relation to the use of legitimate interests as a basis for Processing, in particular in relation to Article 13.

General requirements (Articles 14 – 21)

32. Article 14 imposes obligations on both Controllers and Processors in relation to the protection of Personal Data through technical and organizational measures. Systems should, by default and design, protect the rights of Data Subjects.

33. All Controllers must implement and maintain an appropriate written data protection policy. The obligations binding on Processors under Article 14 include the requirement to implement and maintain an appropriate written data protection policy where proportionate in relation to the Processing activities. In other words, a Processor who carries out only small-scale incidental Processing, for example, may not require a written data protection policy as a matter of law. Nevertheless, it would be good practice for all Processors to have a policy.

34. Controllers must maintain general written records, as required by Article 15. Each Processor must maintain a record in relation to each specific Processing activity it undertakes.

35. Controllers and Processors who undertake High Risk Processing Activities systematically, regularly or by necessity must appoint a DPO (data protection officer). Generally, the DPO should be resident in the UAE; however, we are conscious that where organisations are part of larger groups there may be a DPO (or similar) already within the group outside the UAE who could perform the role, so the Proposed Law allows for this. The provisions of Articles 17 and 18 relating to the competence, status, position and tasks of the DPO must be complied with in any event. The DPO will be required to complete an annual assessment and submit the same to the Commissioner of Data Protection. This is not intended to be an onerous obligation and will be integrated into existing DIFC compliance and reporting cycles.

36. Article 20 requires data protection impact assessments to be performed by Controllers where High Risk Processing Activities are to take place. Where the Processing activity is substantially the same as Processing activity conducted by another member of the Controller's Group, and another member of the Controller's Group has conducted an impact assessment which complies with the requirements of the Proposed Law, the

Controller may rely on such assessment. There is a further exception for Processing based on certain grounds related to compliance with Applicable Law.[2]

37. A Processor should assist with a data protection impact assessment where the Processor has been appointed by the Controller to carry out the Processing in question or is in discussions with the Controller (which are not merely hypothetical), with a view to being so appointed.

38. Controllers must consult with the Commissioner of Data Protection where a data protection impact assessment under Article 20 indicates that the risks to the rights and freedoms of Data Subjects remain particularly high and the Controller has already carried out or wishes to commence or continue with the Processing activity.

39. Controllers with common interests in certain Processing activities (for example, an industry group) may commence joint consultation with the Commissioner of Data Protection.

Q6. Controllers and Processors are invited to raise any concerns in relation to the record keeping requirements in Article 15.

Q7. Is the definition of High Risk Processing Activity sufficiently clear? We ask Controllers and Processors to bear in mind that, in practice, if such persons are in any doubt as to whether their activities are High Risk, our intent is that they would adopt a cautious approach and appoint a DPO. In due course, the Commissioner may publish guidance or Regulations which confirm (non-exhaustively) that certain types and categories of Processing operations are considered to be High Risk Processing Activities.

Q8. If you believe you will be required to appoint a DPO but have concerns about your ability to do so, please provide details.

Q9. We welcome the views of Controllers as to whether the requirements in relation to the need to carry out a data protection impact assessment are clear.

Q10. In certain circumstances described in Article 21, a Controller may be required to consult with the Commissioner of Data Protection. We welcome the views of Controllers as to whether the requirements in relation to the need to consult are clear.

Cessation of Processing (Article 22)

40. The Proposed Law contains the requirement for Controllers to delete or to put beyond use Personal Data where the basis for Processing such Personal Data ceases to exist or the exercise of a Data Subject right compels such action. There is an exception to this requirement where the Personal Data are needed in relation to the establishment or defence of legal claims or where the Personal Data are needed for compliance with Applicable Law.

[2] See Article 20(9).

Q11. The concept of putting data "beyond further use" is included in recognition of the fact that some storage systems, Processing methods or technologies which can legitimately be used present difficulties when it comes to permanent and complete deletion of data.

We welcome opinions from Controllers as to whether the definition of "beyond further use" in Article 22(2) is clear.

We would like to hear from Controllers currently Processing Personal Data who believe that such Personal Data can be neither deleted nor put "beyond further use" (as defined) when the basis for Processing ceases to exist. We would be keen to understand such circumstances in more detail and request Controllers to provide as much information as possible (respecting confidentiality and privacy); alternatively, we would be happy to discuss such matters directly with Controllers.

Joint Controllers (Article 23)

41. The Proposed Law contains the concept of Joint Controller.

42. Joint Controllers must, by written agreement, detail how they will ensure compliance with the Proposed Law, in particular how they will interact with Data Subjects (in terms of the information requirements and the handling of Data Subject requests to exercise rights). Such agreement may be contained within a broader agreement.

43. With respect to the liability of Joint Controllers under the Proposed Law: Data Subjects may exercise rights against any of the Joint Controllers and the Joint Controllers are all responsible for ensuring all applicable Controller obligations (relating to the Personal Data in question) are complied with. There is nothing to stop Joint Controllers agreeing indemnities and other risk allocation provisions between themselves.

44. If the Joint Controllers violate the Proposed Law and are subject to administrative imposition of fines under Article 62 then the Commissioner of Data Protection may apportion such fines between the Joint Controllers in whatever manner the Commissioner of Data Protection deems just to take account of their respective culpability for the violation.

Q12. Controllers who believe they may be Joint Controllers may provide comments on Article 23.

Processors (Article 24)

45. Article 24 requires Controllers to ensure that Processors which are engaged provide sufficient commitments to protect Personal Data. The Article places controls on the appointment of sub-Processors. The Article requires arrangements between a Controller and a Processor (and between Processors) to be governed by a legally

binding contract in writing containing certain provisions (which are closely aligned to the latest legal contracting requirements in relation to personal data processing contracts). Both Controllers and Processors are in violation of the Proposed Law if they commence the Processing activities without a binding written agreement being in place which complies with the Proposed Law.

46. The Commissioner of Data Protection may endorse or provide a certain form of words which meets the requirements of Articles 24(3) and/or 24(4). Such form of words is not intended to be the only compliant form of words and use of such form is not mandatory.

As written, from the moment the Proposed Law becomes effective, the Proposed Law provides that all arrangements between Controllers and Processors must comply with Article 24 otherwise such parties will be in violation of the Proposed Law. It is acknowledged that this presents problems with respect to arrangements already in place before the Proposed Law becomes effective. In Europe, for example, much time and effort was spent "remediating" existing contracts for GDPR, sometimes with uncertain legal results (where both suppliers and customers purported to impose their own terms). Ultimately, it is not (usually) wholly within the gift of a single party to amend the terms of an agreement so even parties which conscientiously sought to comply with updated international data protection laws such as the GDPR could not ensure their own compliance in the absence of agreement from counterparties.

Q13. As noted, the Commissioner of Data Protection may publish model contract clauses to assist Controllers and Processors. Could Controllers and Processors please confirm if the publication of model clauses by the Commissioner of Data Protection would be helpful – in principle – in ensuring a smooth process of contract amendment without the need for a "battle of the forms" or for protracted negotiations? Such clauses would not address liability limitations or exclusions.

Q.14 We are prepared to consider a reasonable transitional period during which existing agreements would not be deemed to be in violation of the Proposed Law, subject to suitable parameters. We would certainly expect significant Processing agreements (where high volumes of Personal Data are involved, where Special Categories of Personal Data are involved or where the Processing is high-risk for some other reason) to be amended to ensure compliance as soon as possible. We welcome comments from both Controllers and Processors on the following:

- the number of arrangements that the party believes they would need to address (to allow us to form a view of the compliance burden on such parties);
- what proportion of the arrangements are significant Processing arrangements;

Data Export (Articles 26 – 28)

47. Provisions regarding transfers out of the DIFC to a jurisdiction providing adequate levels of data protection are similar to under the Current Data Law. In due course, the Commissioner of Data Protection shall reconfirm which jurisdictions provide adequate levels of data protection.

48. Regarding provisions which relate to the transfer of Personal Data to a Third Country (i.e. a jurisdiction not deemed to provide adequate levels of data protection), we would

like to draw the attention of Controllers to the word "necessary" in Articles 27(3)(b) to 27(3)(g) and also in 27(3)(j) and 27(3)(k). It is not intended that Article 27(3) is the "go-to" provision to legitimise Personal Data transfers to Third Countries. Controllers should always endeavour to implement safeguards in accordance with Article 27(2). Article 27(3) is, in general, intended to provide a practical means for effecting specific transfers where Article 27(2) safeguards cannot be implemented. Controllers should be mindful that the need to protect, and respond to the exercise of, Data Subject rights is better served by reliance on Article 27(2) than on Article 27(3).

49. Under the Current Data Law it is permitted to transfer Personal Data to a Third Country to comply with audit and accounting requirements. This specific permission has been removed on the basis that there is no reason why such transfers of Personal Data (if necessary) cannot be conducted in accordance with one of the safeguard mechanisms specified in Article 27(2) or, potentially, under Article 27(3) on specific occasions.

50. There is also a limited further exception permitting transfers to Third Countries set out in Article 27(4).

51. Public authorities should note Article 27(5).

52. Article 28 regulates how Controllers must manage requests from official authorities for the disclosure of Personal Data outside the DIFC. We recognise that Controllers may otherwise be placed in a position of conflict between the requirements of the Proposed Data Law and the requirements of other Applicable Law to which the Controller may be subject. We have attempted to provide a practical and workable regime.

Q15. Controllers who expect to fall within the scope of Article 28 are invited to provide comments on the Article.

Provision of Information (Articles 29 - 31)

53. These Articles require Data Subjects to be provided with information. The Articles specify the required information and conditions in relation to the presentation and delivery of the information which are broadly consistent with GDPR.

54. The Commissioner of Data Protection is aware that Processing technologies and methodologies evolve. Some Processing technologies may be difficult to reconcile with the potential exercise of Data Subject rights. Under the Proposed Law, there are limited circumstances, predicated on the nature of the Processing activity, in which Controllers can lawfully refuse to comply with a request from a Data Subject to exercise his or her rights. Such circumstances are referred to in section 56 below. It is a key principle, however, of the Proposed Law that a Controller may only reject the exercise of a Data Subject's right (in the permitted circumstances) if the Controller provided sufficient notice to the Data Subject initially which made it clear to the Data Subject that such right would

be impacted by the Processing activity. Article 29(1)(g)(ix) contains the relevant information provision requirement.

We are keen to consult on the issues noted in section 54, which are not addressed in other prominent data protection laws. Please see question 16 below.

Data Subject Rights (Articles 32 - 40)

55. The Proposed Law provides the following Data Subject rights:

(a) withdrawal of consent (absolute right, subject to limited exceptions created by operation of law);

(b) right of access (absolute right, subject to limited exceptions created by operation of law);

(c) rectification (absolute right unless not technically feasible and the Controller has complied with Article 29(1)(ix));

(d) erasure (right conditional on certain criteria as per Article 33(2));

(e) right to object (right to object is absolute but the consequences of an objection do not follow automatically; see Articles 34(2) to 34(4));

(f) right to restrict Processing (the extent of the restriction is limited by the Proposed Law and the right is exercisable only where certain criteria apply; see Article 35);

(g) right to portability (applies only in certain circumstances; see Article 37);

(h) right not to be subject to a decision based solely on automated Processing, including Profiling, which produces legal effects or similarly significantly affects the Data Subject (right conditional on criteria applying; see Article 38); and

(i) non-discrimination (absolute right, unless discrimination is for objectively valid commercial grounds; see Article 39).

56. The Commissioner of Data Protection recognises that Data Subject rights of rectification; erasure; and, objection, may not be easily compatible with certain manners of Processing. The Commissioner of Data Protection's current view is that, so as not to cause tension between legal duties and rights and the proper desire of business to innovate and responsibly use new technologies, such Data Subject rights can be lawfully rendered un-exercisable provided that sufficient information or notification is provided to the Data Subject by the Controller at the outset to enable the Data Subject to weigh up the pros and cons of the Processing and reach an informed decision. With respect to the right to rectification, it is also acknowledged that inaccurate Personal Data may have

adverse impacts on a Data Subject. Where the inaccuracy was not the Data Subject's own doing (by providing inaccurate data to the Controller) the Controller is required to provide all reasonable assistance to the Data Subject if the Personal Data cannot be rectified. Please see Articles 33(4), 33(5), 34(4) and 29(1)(g)(ix).

57. Controllers should note the Data Subject rights which are absolute and not subject to further conditions (withdrawal of consent and access). Controllers should not Process Personal Data in a way which is incompatible with such rights. Given that withdrawal of consent to Process Personal Data may mean that Personal Data needs to be deleted or put beyond use, Controllers should note that relying on consent as a basis for Processing Personal Data is unsatisfactory when the Processing method in question will make deletion of Personal Data impossible or infeasible.

Q16. Controllers who intend to use innovative Processing methods where erasure (and therefore complying with a valid objection) and rectification (for example, where stored Personal Data are intended to be immutable) are technically impossible or infeasible are invited to provide views on the provisions referenced in section 56.

Breach notification (Articles 41 and 42)

58. Controllers may be required to notify Personal Data Breaches to the Commissioner of Data Protection and to affected Data Subjects. Controllers should note that it is not-mandatory to notify every Personal Data Breach and there are qualitative thresholds in both Article 41 and 42 which need to be met before the obligation arises.

Commissioner of Data Protection (Articles 43 – 58)

59. These Articles contain numerous administrative provisions which are largely similar to the corresponding provisions of the Current Data Law.

60. Articles 50 and 51 relate to certification schemes and certification bodies, to enable Controllers and Processors to demonstrate compliance with the Proposed Law.

Q17. We are keen to hear from any Controllers or Processors who believe certification schemes would be valuable and from any person who has an interest in establishing a certification scheme and being recognised as an approved certification body. Please provide your comments.

Remedies, Liabilities and Sanctions (Articles 59 – 64)

61. The basic principles and operational mechanics of these sections are largely unchanged from the Current Data Law.

62. It should be noted that the schedule of fines in the Current Data Law is considered inappropriate for the Proposed Law. The Commissioner of Data Protection believes that a highly granular approach to setting maximum administrative fine limits may drive the wrong behaviours as breaches of the law can be "priced". The Commissioner of Data

Protection also notes, however, that the adverse effects of being found to violate the Current Data Law and the Proposed Law (reputational damage, increased scrutiny from other competent authorities, Data Subject compensation liability) extend beyond liability for administrative fines. The Commissioner of Data Protection further notes that any administrative fines should be proportionate to the nature and scale of any violation of the law, including the actual harm caused to Data Subjects. In due course, the Commissioner for Data Protection may elect to make Regulations to clarify the parameters of potential administrative fines.

63. It should be noted that Data Subjects are entitled to compensation under Article 64 if material or non-material (for example, distress) damage is caused by a contravention of the Proposed Law. This is consistent with the position under the GDPR.

64. Under Article 64(2), Processors are only liable to compensate Data Subjects for the damage caused by Processing where the Processor has breached an obligation directed at Processors or has acted outside or contrary to the lawful instructions of the Controller.

65. Under the GDPR, Article 82(3) provides that a Controller or Processor is exempt from liability for the damage caused by Processing if it proves that it is not in any way responsible for the event giving rise to the damage. The meaning of that Article is unclear in practice (particularly from the perspective of the Controller) and may be settled by court precedence over time. The Commissioner of Data Protection does not think that reflecting the same principle in the Proposed Law will be helpful. The Commissioner of Data Protection believes that Controllers should be legally responsible to Data Subjects for all Processing; this provides certainty for Data Subjects and the Commissioner of Data Protection is also mindful that Processing activity may be performed by a Processor incorporated outside the DIFC and that enforcement of a judgment against such Processor may be difficult. It is open for proceedings to be brought against Processors under Article 62(2) if the complainant elects to do so or for Controllers to apply for Processors to be joined in proceedings in such circumstances.

66. If Controllers are concerned about assuming liability as a result of the act of a Processor then appropriate contractual provisions can be agreed to enable Controllers to recover losses from Processors.

Q18. Controllers and Processors are invited to comment on the provisions of Articles 59 – 64.

General Exemptions (Article 65)

67. DIFC bodies entitled to exemption under the Current Data Law retain entitlement to exemption under the Proposed Law, however under the Proposed Law the exemptions are not broad and automatic and must be justified on a case-by-case basis. The Commissioner of Data Protection will assess case-by-case exemptions.

Legislative Proposal

68. This legislative proposal contains the following:

(a) the Proposed Law (at Annex A);

(b) a table of comments to provide your views and comments on the consultation paper (at Annex B).