DIFC

CONSULTATION PAPER NO. 2

April 2023

Amended Data Protection Regulations

CONSULTATION PAPER NO. 2
AMENDED DATA PROTECTION REGULATIONS

Why are we issuing this paper?

1. The Dubai International Financial Centre Authority ("DIFCA") proposes to enact amended Data Protection Regulations (the "**Proposed Regulations**") to establish additional areas of regulation that support robust implementation of the Data Protection Law, DIFC Law No. 5 of 2020 (the "**DPL**"). This Consultation Paper No. 2 of 2023 ("Consultation Paper") seeks public comments on the Proposed Regulations.

Who should read this paper?

2. This Consultation Paper would be of interest to persons conducting or proposing to conduct business in the DIFC. In particular:

   a. Data protection officers, professionals, and the senior managers of the companies they represent;

   b. Landlords of leased offices in the DIFC;

   c. Developers of technology that enables the digital economy;

   d. Marketing and communications professionals and the companies they support; and

   e. legal advisors to any of the above.

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.

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.

What happens next?

6. The deadline for providing comments on the proposals in this Consultation Paper is 17 May 2023.

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

8. The Proposed Regulations are in draft form only. You should not act on them until they are 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, or are defined in the DPL or the Proposed Regulations. Unless the context otherwise requires, where capitalisation of the initial letter is not used, the expression has its natural meaning.

Background

I. Regulation 8: Personal Data Breaches

10. Article 41 and Article 42 of the DPL address Personal Data Breaches. Due to the potentially sensitive nature of the Personal Data that may be exposed by way of a Personal Data Breach, it is important to lay down regulations to clarify the actions and remedies required to report and manage such an incident.

11. In certain instances, a Personal Data Breach may occur where a former tenant of a DIFC-based property accidentally or intentionally leaves information behind that contains or potentially contains Personal Data ("**Inadvertently Obtained Information**").

12. Upon consideration of independent legal consultation and advice, the Proposed Regulations seek to address the steps necessary to assess whether a Personal Data Breach has occurred regarding Inadvertently Obtained Information and what actions, if any, the Commissioner may consider to assure that fair and lawful processing and remediation occurs thereafter.

II. Regulation 9: Data Collection and Use for Digital Communications and Services

13. Collection and use of Personal Data for use in electronic marketing or general outreach, along with Personal Data and consent collection through website interfaces for the provision of various digital services ("**Digital Communications and Services**") are addressed generally in the DPL and specifically in obligations included in Articles 12, 14(4), 22, 29(1)(h)(viii) and (ix), 30, and 31.

14. Personal preferences and ability to control the use of one's Personal Data after it has been shared, even if apparently voluntarily or publicly, is a basic privacy right that the DPL obliges companies in the DIFC and elsewhere to adhere.

15. Regulation 9 is proposed in order to provide clear collection, use, and lawful basis requirements regarding Digital Communications and Services. These regulations will reinforce the accountability and transparency of DIFC-based entities in such situations. They will also enhance the objectives of the DIFC to continuously evolve as a jurisdiction that enables digital economy through an efficient legal structure protecting consumers from intrusive, unlawful digital data practices as well as companies that implement such regulations from potential risk of enforcement action imposed by other regulatory authorities.

III. Regulation 10: Personal Data Processed Through Digital Enablement Technology Systems

16. It is becoming increasingly important to provide controls and guardrails around Personal Data collection and use for processing in a variety of new ways, including via platforms built through digital enablement technology systems such as artificial intelligence ("**Systems**").

17. While such Systems are a powerful and useful tool in daily life, the amount of Personal Data processing that occurs to power them is exponentially more than that used in any other technology that came before them.

18. In addition, these Systems are increasingly designed to be "generative", meaning they are built to generate volumes of data, including audio, code, images, text, and much more. They are also designed to learn how to Process Personal Data through a variety of instructions and patterns for uses and results that are derived from such instructions. Generative machine learning or enablement is potentially extremely useful in terms of positive outcomes such as sustainability, transparency, accountability, and improving quality of life. At the same time it is potentially extremely dangerous in terms of resulting unwanted bias, controversial political or financial implications, or in impressions or directions of actions that negatively impact the data subject himself.

19. Implementing basic technical, organisational, and ethical obligations of Controllers and Processors are the starting point for "regulating" any types of generative, machine-learning, large language model Systems. This is because they are still a vastly unknown quantity but the ability to assert controls and concepts in order to direct the Processing and mitigate risk is not.

20. Until such Systems and use cases are better understood, setting out regulations reinforcing relevant controls and concepts to fairly and ethically develop them is of immediate concern.

21. Regulation 10 addresses these obligations, controls and concepts, incorporating requirements that ensure compliance with critical parts of the DPL, including fair and lawful processing, and human intervention when input queries may result in responses that ought to be designed to share Personal Data with government authorities in line with Article 28 of the DPL.

Key features of the Proposed Regulations

22. The key aspects of the proposal include the:

(a) directions for a DIFC-based entity or landlord to follow to determine whether a Personal Data Breach has been committed, whether by the company itself or by a previous tenant, and if or when to report such breach;

(b) accountability and transparency controls and processes for assuring data subjects' rights if their Personal Data is collected and used for digital communications and services by a DIFC-based company;

(c) clarity on the obligations of Controllers and Processors regarding controls and safeguards to be built into digital enablement technology systems; and

(d) concepts to incorporate privacy by design or default into generative, machine learning or similar Systems

Regulation 8: Personal Data Breaches

23. It is potentially unclear whether a finder of Inadvertently Obtained Information that potentially or does in fact contain Personal Data becomes a Controller or Processor of such data.

24. It is also necessary to ascertain what should be done with such Inadvertently Obtained Information and who ought to make that decision.

Q1. What are your views on whether a Party that finds Inadvertently Obtained Information that potentially contains, or does in fact contain, Personal Data becomes a Controller or Processor of such data?

Q2. Do you think any other criteria for the Party that finds Inadvertently Obtained Information to make this determination is necessary or desirable?

Q3. Is it appropriate for the Commissioner of Data Protection to make a determination and associated directions (if any) regarding disposal / disposition of such data?

Q4. Please comment on the fairness, necessity and proportionality of the requirements set out in Regulation 8.4.6.

Q5. Please comment on the fairness, necessity and proportionality of the requirements set out in Regulation 8.4.7.

Regulation 9: Collection and Use of Personal Data in Digital Communications and Services

25. Understanding the nuanced and often risky territory of use of Personal Data in Digital Communications and Services is the objective of proposed Regulation 9.

26. Alignment of proposed Regulation 9 with international best practices and obligations is a further objective, in order to diminish fragmentation.

Q6. Are the proposed requirements set out in Regulation 9 clear regarding appropriate collection, use, notification and rights obligations when engaging in Digital Communications and Services provision? If not, please provide a detailed explanation for your views.

Q7. Will proposed Regulation 9 mitigate risks to companies that are required to also comply with international obligations in this area of practice?

Q8. Will proposed Regulation 9 mitigate risks to Data Subjects regarding their rights to control the use of their Personal Data, especially in the context of Digital Communications and Services?

Regulation 10: Personal Data Processed Through Digital Enablement Technology Systems

27. Digitisation of our every day functions and the immense power of the technology that creates platforms for this purpose also requires controls to and guideposts to establish etiquette and ethics around its development.

28. Whereas many jurisdictions are attempting to promulgate principles, frameworks and in some cases regulating the content and composition of algorithms themselves for this purpose, proposed Regulation 10 seeks to take a small but important first step in establishing boundaries for Controllers and Processors vis a vis emphasising the relevant requirements of the DPL, including but not limited to:

a. Prompt and clear notification requirements relevant to Systems development and use;

b. Encouraging the use of applicable codes or standards; and

c. Incorporation of such principles to assure that negative impacts to the rights of Data Subjects are minimised or eliminated through well-formed, human-centric standards for algorithm development.

29. On this basis, it is suggested that related guidance on this Regulation comprised of use cases, case studies and specific information serves to provide the foundational support for further regulation on this topic, that then grows over time.

Q9. Does the approach proposed in Regulation 10 of "regulating" Systems through data protection principles for collection and use of Personal Data serve as a reasonable starting point for setting basic controls around Processing in this manner? If not, please provide detailed reasons.

Q.10 Would this approach assist in mitigating risks of harm to individuals whose Personal Data is processed? If not, please provide detailed reasons.

Q.11 Would this approach to regulation assist designers of Systems with understanding and implementing controls by design and default, while permitting flexibility for innovation? If not, please provide detailed reasons.

Q.12 What other approaches would you suggest? Please provide detailed responses.

Q.13 Should a common set of principles regarding such Systems be agreed at an international level, and if so, what governmental or non-governmental body would be most appropriate to do so? Please provide detailed responses.

Q.14 What other questions or issues should be asked and addressed in the Regulations or guidance?