REGULATION 10 ON PERSONAL DATA PROCESSED THROUGH AUTONOMOUS AND SEMI-AUTONOMOUS SYSTEMS

Commissioner of Data Protection

DIFC

CONTENTS

DIFC

1. Introduction

The goal of the DIFC Commissioner of Data Protection (the **Commissioner**) in producing this guidance is to assist Controllers and Processors subject to the Data Protection Law, DIFC Law No. 5 of 2020 (the "DPL") and the Data Protection Regulations issued pursuant to the DPL (the "Regulations") about implementation of Regulation 10 on Personal Data Processed through Autonomous and Semi-Autonomous Systems (“Regulation 10”).

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 has been adapted from and may be read in conjunction with existing UK guidance where available.

*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. Regulation 10: Background and Objectives

Clarifying the regulations issued regarding the processing of Personal Data through autonomous or semi-autonomous systems, broadly, artificial intelligence or "AI", which encompasses various subsets, including machine learning, deep learning, neural networks, natural language processing, and genetic algorithms, is important to any DIFC business that is using or plans to use such technology (and other emerging technologies).

First and foremost, applying Regulation 10 requirements may act as a further organisational measure to integrate into a robust data protection compliance program vis a vis the DIFC DP Law. Given the number of X-tech and Innovation Hub entities developing complex software using or itself being AI-based, the Commissioner's objectives in issuing regulations, conducting use case testing in a sandbox environment and developing detailed guidance therefrom are to better protect the Personal Data that forms the core of most processing operations. Further, it protects the rights of data subjects to understand and, to the extent possible, control how their data is processed.

For instance, Regulation 10 activates a key protection provided for in the DP Law 2020 that until now has had limited exposure – that is, Article 29(1)(h)(ix), which states that where advanced technology is deployed that does not permit the exercise of data subjects' rights such as erasure, the deployer / controller must provide sufficient notice in that regard and satisfy itself that the data subjects understand the impact. Apart from this article's unique character as setting out government data sharing protocols within a data protection law, the regulation implementing it will provide that much more clarity on the importance of notice, choice, and accountability when a system is deployed. In using Personal Data and being designed to potentially take on a life of its own, effectively, a System can be wildly useful to productivity and accuracy, but may also cause damage if not carefully monitored and its functions reported on. To this end, Regulation 10 sets out requirements to address these challenges, for example, maintaining a register of AI processing activities, at least, again, to provide an accountability and transparency measure and a basic map for warp speed processing.

Another key feature of Regulation 10 is that it creates space for DIFC to be a platform for interoperability of guidelines and principles in an environment where national governments and organisations are developing their own. Regulation 10 allows for a "plug and play" environment, where *any* template principles, within reason and subject to consultation if requested by the Commissioner, can form the basis of generative technology development. Regulation 10 gives a wide berth for AI principles forum choice, providing flexibility to the developer or Deployer, Operator or Provider, while ensuring at least an accepted set of principles are applied in the logic.

Regulation 10 for now only has the processing of Personal Data in such systems in scope. It is outcomes-based, and looks to practical risk prevention procedures to safeguard Personal Data. Inherent in this approach is that a Deployer, Operator or Provider in its capacity as a Controller must by law assess whether it is conducting High Risk Processing even before the system has a chance to see the light of day, and take appropriate actions to:

- control the processing environment both at home and outside of the DIFC in terms of import and export of Personal Data
- apply additional safety measures
- appoint a Data Protection Officer and / or Autonomous Systems Officer
- assess ongoing risks of processing in such Systems

- most importantly, provide credible evidence of privacy by design in the Systems they develop, deploy or operate.

Note as well that Regulation 6.2, Unfair or Deceptive Practices, has a direct impact on Regulation 10, which is worth discussion in this context. Such practices may include misleading notices of processing activities or public representations regarding certifications or adherence to principles, codes and compliance standards. All of these measures go to ensuring that the Deployers, Operators and Providers of Systems stay focused on the evidentiary and transparency requirements under Regulation 10 through clear, demonstrable documentation and cooperation with the Commissioner's Office or any other relevant supervisory authority.

DIFC's outcomes-based risk assessment and evidentiary approach vis a vis application of the DP Law 2020 obligations to the development and use cases for Systems provides a more collaborative, transparent way of creating and maintaining an innovative yet safe System. This guidance provides interpretation of the "Guidance notes" within Regulation 10 as a starting point and will develop over time to include use cases and updates based on them.

4. Regulation 10.1: Autonomous and Semi-Autonomous Systems

4.1 Regulation 10.1

Guidance note:

Because a System is itself comprised of data (e.g., the program code of the System), to the extent that a System resembles the physical appearance or behaviour of an Identifiable Natural Person (irrespective of whether the System has been specifically designed or trained to achieve such resemblance, or such resemblance is unintended), then the use or operation of that System (for any purpose and in any manner, and including in circumstances where the System is not used to Process any Personal Data) will be itself considered Processing of Personal Data about that Identifiable Natural Person subject to the Law.

Interpretation:

As Systems develop and permutations grow without supervision in most cases, it is possible that the term "taking on a life of its own" really occurs. This is especially true where the System begins to act and even holds itself out as a person and in some cases as an existing person whose data would be ordinarily covered by the DP Law 2020. As such, processing that occurs in this context will be caught by the DP Law 2020, and the Deployer, Operator or Provider of the System will be accordingly accountable.

4.2 Regulation 10.1.1(a)

Guidance note:

The definition of System has been adapted on the basis of the OECD guidelines and the draft Regulation of the European Union on harmonized rules on AI ("EU AI Act") to encompass systems that are capable of autonomous or semi-autonomous operation. The Law already contains provisions governing the use of automated Processing, so it is not intended that purely automated systems (i.e. systems which have no degree of autonomy in their operation and whose operation is deterministically controlled by humans) should be captured in this definition. With respect to the reference to Personal Data in Regulation 10.1.1(a) , it is anticipated that the definition of Personal Data could be broadly interpreted to encompass identification of virtual personas or similar virtual criteria that identify an individual.

Interpretation:

Avatars or other virtual personas that are representative of a living Identifiable Natural Person may be interpreted as Personal Data and as such, the DP Law 2020 will apply accordingly in this context.

4.3 Regulation 10.1.1(b)

Guidance note:

The concepts of a "Deployer" and "Operator" of a System have been introduced to address the potential problems of applicability of the traditional concepts of a "Controller" and "Processor" in circumstances where no person can be said to be, strictly speaking, "in control" of the processing or "determining" the purposes of the processing. The definition of "Deployer" has been adapted from the eponymous concept in the EU AI Act as well as the concept of "user" in the draft Management Measures for Generative AI Services promulgated by the Cyberspace Administration of China. The approach adopted in this Regulation is to assign the general responsibilities of a traditional "controller" to the person or entity that authorizes or benefits from the operation of the System and any output it produces, in order to make the "Deployer" generally accountable for its compliance with the Law.

Interpretation:

Due to certain unquantifiable factors in developing, deploying or operating Systems that change the nature and qualities of a Controller or Processor of Personal Data to a certain degree, i.e., through a machine becoming the Controller or Processor rather than a legally identifiable entity that carries out these functions, this regulation can be interpreted to apply the values accordingly, as determined by the Commissioner based on the circumstances.

4.4 Regulation 10.1.1(c)

Guidance note:

By analogy with the concept of a "Deployer", the concept of an "Operator" of the System is introduced to ensure the technical service provider acting on the instructions and for the benefit of a "Deployer" is accountable to the same extent and substantially in the same manner as a traditional "processor".

Interpretation:

No further interpretation necessary at this time.

5. Regulation 10.2: Obligations of Deployers and Operators of Systems

5.1 Regulation 10.2.1

Guidance note:

Both the "Deployer" as well as the "Operator" of a System must comply with the general requirements for legitimate and lawful processing under the Law in substantially the same manner as a traditional "controller" and "processor".

Interpretation:

No further interpretation necessary at this time.

5.2 Regulation 10.2.2(a)

Guidance note:

This requirement implements the principle of transparency and is consistent with analogous requirements implemented in the draft EU and Chinese regulations on the use of AI. Transparency is a fundamental element of the regulatory scheme adopted in Regulation 10 and ensures that concerned individuals who may be impacted by the use of AI in the processing of their Personal Data are not only made aware of the use of a System, but also provided sufficient details to enable them to make an informed assessment of the risks and ultimately decide whether to take steps to object or withdraw the legal basis permitting the processing by the System.

Interpretation:

Regulation 10.2.2(a) and Article 29(1)(h)(ix) lay the groundwork for ethical, responsible and safe use of advanced technology through the one thing that data subjects should be able to rely on to understand the bases and purposes for collecting and processing Personal Data: direct notice to the individual.

One of the key objectives in the promulgation of DP Law 2020 was to ensure that when technology was capable of negatively impacting data subjects' rights, the DP Law would account for and make Controllers accountable for, ensuring the impact is as minimal as possible. Article 29(1)(h)(ix) was developed for precisely this purpose.

Regulation 10.2.2(a) mandates that particularly in the context of an advanced, machine learning and generative System, transparency regarding what an individual can and cannot control when their data is processed vis a vis such System is vital. Full transparency might not always be possible and disclosing information could exacerbate risks. However, where feasible, transparency coupled with understanding the functionality and capabilities around effective exercise (or lack thereof) of data subjects' rights may prevent an individual user of the System from sharing information that they do not want onward transferred, exposed, or made indelible, as such Systems are prone to, or from using the System all together. This is especially relevant in the case of generative AI. Without these fundamental choices being provided to through sufficient notice and risk assessment of the data subject's comprehension of the notice, irreversible damage may result.

5.3 Regulation 10.2.2(b)(i) – (v)

Guidance note:

The regulatory scheme adopted in Regulation 10 categorizes the purposes for processing of Personal Data by a System as either "human-defined", that is purposes that are externally pre-defined by humans and "hard coded" into the System, which the System cannot change, or "self-defined" (i.e., purposes which the System is able to generate itself). Any purposes for processing which the System is capable of dynamically generating itself must be contemplated on the basis of an exhaustive set of detailed principles, that are themselves externally predefined by humans and "hard coded" into the System, and which the System cannot change.

Interpretation:

Human-defined processing purposes must always prevail in Systems development and use, even if the System itself if capable of taking on a life of its own and defining purposes as the logic progresses to a conclusion. The capability of a System to at any point self-defined processing purposes must derive from human-defined principles and objectives. Demonstration of self-defined processing purposes capability will necessarily lead to exercise of the request for such evidence under the relevant provisions of Regulation 10.

5.4 Regulation 10.2.2(c)

Guidance note:

The regulatory scheme adopted for Regulation 10 is premised on a permissive certification-based regime for the use of Systems to process Personal Data, rather than requiring that any licenses or registrations be made or obtained from the Commissioner. It is anticipated that the Commissioner will, in future guidance, establish certification requirements that apply to Systems used generally in the processing of Personal Data, as well as additional or different requirements applicable specifically to Systems that are used in High Risk Processing Activities involving Personal Data.

Interpretation:

Unless a certification requirement or regime is presented to the Commissioner for adoption in a specific System use for processing, certification requirements are open for interpretation and otherwise will be considered and updated in future, separate guidance. Please consult with the Commissioner's Office for further guidance or queries.

6. Regulation 10.3: General Requirements for Autonomous and Semi-Autonomous Systems

6.1 Regulation 10.3.1(a) – (e)

Guidance note:

This provision gives force to the fundamental principles of fairness, ethical compliance, transparency, security of operation and accountability that each System that is used to process Personal Data must ultimately comply with. The regulatory purpose of the provision is to establish these principles as overarching requirements that Systems must be designed to comply with. However, the provision purposefully does not limit its application to "Developers" of Systems only, because it anticipates that ultimately it may be "Deployers" and "Operators" that, being the visible entities with direct exposure to any data subjects impacted by the operation of the System, must be held accountable for compliance. "Deployers" and "Operators" would then ensure in turn that they procure Systems only from "developers" that can give them contractual comfort of compliance-by-design with these principles.

Interpretation:

Based on the Commissioner's review and assessment of common Systems principles as noted Regulation 10.2.2(b)(5), the concepts in Regulation 10.3.1(a) – (e) when implemented in any System development provide sufficient comfort and flexibility, while supporting innovation and responsibility.

This regulation also creates a "plug and play" environment of interoperability, allowing reasonably promulgated "principles" from other organisations or jurisdictions to be applied rather than mandating consideration of yet another set of principles. This approach lends itself to fair, pragmatic application of the issues that impact the larger political and social discussion around the digital, AI-driven economy.

6.2 Regulation 10.3.2

Guidance note:

It is anticipated that the Commissioner will establish, in future guidance, general certification and other requirements applicable to Systems used in the processing of Personal Data. When such requirements are established, all Systems must comply with them. In addition, Systems that are capable of dynamically defining for themselves further purposes of processing must do so strictly within the limits and on the basis of the principles "hard coded" into them by human action.

Interpretation:

No further interpretation necessary.

6.3 Regulation 10.3.3

Guidance note:

Given the special nature of High Risk Processing Activities, it is intended that only Systems that fully comply with the specific certification and other requirements established by the Commissioner in future guidance may be used for any High Risk Processing Activities. Furthermore, it is the regulatory intent that no System may be used for High Risk Processing Activities until the Commissioner has promulgated these certification and other requirements.

Interpretation:

Interpretation and application of Regulation 10.3.3 may be considered by the Commissioner on a case by case basis.

6.4 Regulation 10.3.4(a) – (c)

Guidance note:

The fundamental principle of accountability adopted in Regulation 10 is to assign to "Deployers" of Systems substantially the same responsibilities as traditional "Controllers" and by analogy to "Operators" the same responsibilities as traditional "processors" under the Law. These deeming provisions are essential given the definitions of "Controller" and "Processor" under the Law – a "Deployer" should be accountable for how a System processes Personal Data, even if the "Deployer" does not, strictly speaking, determine the purposes of processing, because it is the "Deployer" who benefits from the operation of the System and under whose authority it operates.

To the extent that a System operates fully or semi-autonomously under the authority and for the benefit of its "Deployer", its position is substantially similar to that of an employee within the "Deployer" organization, and the "Deployer" should be therefore liable for its actions in the same way it may be liable for an employee's actions. As a corollary to that, the "Deployer" will be responsible for ensuring that, when processing Personal Data, the System always operates within the appropriate human-established limits and on the basis of human-established principles, much in the same way the "Deployer" would train and require its employees to process Personal Data on its behalf only in accordance with its privacy policies and processes.

Interpretation:

The deeming provisions of Regulation 10.3.4 support the potentially confusing process of determining the roles of Controller and Processing. This is because until now, without clarification, it is possible that the System itself, or other parties involved in use and deployment of the System, may take on any such role, leaving accountability and transparency obligations unclear amongst themselves and to data subjects.

Please also see comments and interpretation regarding Regulation 10.2.2(b)(i) – (v).

7. Autonomous Systems Officer (ASO)

The ASO initially will perform a similar function to that of a DPO. At this time, however, unless the ASO is in fact also the DPO, the requirements of Article 19, DPO Controller assessment, will not apply to this function, but any other obligations may be applicable, whether directly by law or in terms of globally accepted best practice, i.e., conducting data protection impact assessments, reviewing risks and processing activities with senior management, and making recommendations for better accountability and compliance. Please check back regularly for updates to the interpretation of the requirements of the ASO role.

8. Next Steps: Further Developments and Use Case Testing

Use Case testing in a regulatory sandbox may be undertaken. The resulting feedback and proven case studies will feed further development of Regulation 10, including the usual consultation period, and will subsequently updated accordingly on an on-going basis.

9. Questions and Comments

For further information about Regulation 10 vis a vis the objectives of the DP Law 2020, please review general guidance about Data Protection Impact Assessments, Obligations of Controllers and Processors or High Risk Processing & DPO Appointments, as well as assessment tools to get quick, simple and practical answers about these topics.

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.