DIFC

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

Commissioner of Data Protection

DIFC

CONTENTS

1. Introduction 3
2. Scope 4
3. Regulation 10: Background and Objectives 5
4. General Terms and Concepts 6
5. Accreditation and Certification 9
6. Autonomous Systems Officer (ASO) 11
7. Interoperability 11
8. Next Steps: Further Developments and Use Case Testing 12
9. Questions and Comments 12

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.

This guidance addresses questions about implementation of Regulation 10 of the DIFC DP Regulations, enacted in September 2023 regarding Processing Personal Data in Autonomous and Semi-autonomous Systems.

*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 ("HRP") 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. General Terms and Concepts

Q1: How are the DIFC Data Protection Regulations different to the previous version?

The Data Protection Regulations add onto the previous version of the regulations (i.e., DIFC Data Protection Regulations 2020) and support the DIFC Data Protection Law No. 5 of 2020 ("**DIFC Data Protection Law**") further by providing clarity on:

- investigations and enforcement powers of the Commissioner when a Controller or Processor may employ unfair or deceptive practices (Regulation 6.2);

- personal data breach assessment and reporting obligations, including situations where a temporary custodian finds personal data that has been inadvertently left behind or lost (Regulation 8);

- use and collection of Personal Data for marketing and communications, particularly regarding appropriate notices when employing systems that may impair data individuals' rights to restrict or remove their personal data, default cookies settings and conditions for consent, (Regulation 9); and

- Personal data processed through digital, generative technology systems, including but not limited to artificial intelligence ("**AI**") or generative, machine learning technology, (Regulation 10).

Q2: What is an autonomous or semi-autonomous System?

Regulation 10 of the DIFC Data Protection Regulations refers to autonomous and semi-autonomous systems. These are systems which process personal data for human-defined purposes (i.e., functions pre-defined by the Provider and hard-coded into the system) and/or purposes that the system itself defines. These systems then generate an output as a result of or on the basis of such processing.

This broadly defines AI and encompasses various subsets, including machine learning, deep learning, neural networks, natural language processing, and genetic algorithms across application or websites.

Q3. Does the definition of System align with current conventional understanding of this concept in AI and advanced technology?

The definition of System has been adapted on the basis of the OECD guidelines and the 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 DIFC Data Protection Law already contains provisions governing the use of automated Processing, so it is not intended that purely automated systems (i.e., systems that 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 (bundles of) virtual criteria that identify an individual.

Q4: Are all Systems allowed and/or acceptable?

Regulation 10.3 sets out the requirements (including design requirements, human intervention, etc) for acceptable AI systems.

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.

Q5: What is a Deployer?

The DIFC Data Protection Regulations set out obligations on Deployers and Operators of autonomous and semi-autonomous systems.

The Deployer is a person or entity who:

- has authority or direction over the system's operation;
- is benefiting from the system being operated; or
- receives the benefit of the operation of the system or any output generated thereby,

regardless of whether:

- the system is operated, supervised or hosted by such person or entity; or
- such person defines or determines the purpose of which personal data is processed by such system.

In traditional terms, and similarly, the Deployer can be viewed as a Controller.

Q6: What is an Operator?

The DIFC Data Protection Regulations set out obligations on Deployers and Operators of autonomous and semi-autonomous systems.

An Operator is a Provider that operates or supervises a system on behalf of or for the benefit of and on the direction of a Deployer (regardless of whether the Provider exercises control over the processing of personal data by the system). In traditional terms, and similarly, the Operator can be viewed as a Processor.

For completeness, a Provider is a person or entity who develops or procures a system with a view of providing, commercialising or otherwise making such system available to Operators or Deployers.

Q7: What is a Provider?

"Provider" is a natural or legal person that develops a System, or procures that a System is developed for or on behalf of such person, in each case with a view to providing, commercialising or otherwise making such System available to Operators or Deployers

Q8: If I deploy or operate a System, do I have to inform users?

Yes, if Systems are used to process personal data, for transparency, Deployers or Operators must give clear and explicit notice to users upon the initial use or access to systems. The notice should i. alert users to any technology and processes of the system which may process personal data that is not human initiated, controlled or directed and ii. indicate the impact of the use of the system on the user's right to request rectification or erasure of personal data or right to object to the processing of the personal data.

Such a notice should set out appropriate notice elements particularly around the potentially negative impact on the ability to exercise their rights to control their data, in accordance with Regulation 10.2.2(b).

Q9: What type of evidence do Operators and Deployers need to provide under Regulations 10.2.2 (c) – (f)?

Regulations 10.2.2 (c) – (f) set out the various circumstances where evidence is required to be presented upon request to any affected party. Unless specified by the Commissioner in certain circumstances, evidence can be in the form of policies, governance frameworks, principles frameworks and other documentation which demonstrate the specific requirement.

Q10: What are unfair or deceptive practices?

The Commissioner can investigate and take enforcement against a Controller or Processor where a complaint has been made against them for unfair or deceptive practice/behaviour.

Unfair or deceptive practice/behaviour includes (but is not limited to) misleading:

- notices of processing activities;

- public representations regarding certifications or adherence to principles, codes and compliance standards;

- general principles and requirements of lawful processing (as required under Article 9 of the DIFC Data Protection Law);

- transfers outside the DIFC (Article 26 and 27 of the DIFC Data Protection Law);

- Data Subjects as to whether their Personal Data will be used for direct marketing purposes (Article 29(h)(viii) of the DIFC Data Protection Law); or

- Data Subjects where the processing of their personal data will restrict or prevent them from exercising their right to request rectification or erasure of Personal Data or right to object to the processing of the Personal Data (for example where the processing involves digital, generative technology systems, including but not limited to AI or generative, machine learning technology) by not including a clear and explicit explanation of the expected impact on such rights and not satisfy itself that the Data Subject understands and acknowledges the extent of any such restrictions if the Controller intends to process Personal Data in a manner that (Article 29(ix) of the DIFC Data Protection Law).

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.

Unfair or deceptive practice/behaviour will be determined on a case-by-case basis considering the specific complaint and facts of the investigation.

5. Accreditation and Certification

Q11. Regulation 10.3.3 states that no person may use, operate, provide, offer or otherwise make available for commercial use a System to engage in High Risk Processing Activities set out in Schedule 1, Article 3 of the DIFC Data Protection Law unless (a) the Commissioner has established audit and certification requirements applicable to Systems used in High Risk Processing Activities and (b) the System complies with all such requirements (among other obligations).

A) Is there such an audit and certification framework? Yes, the Regulation 10 Accreditation and Certification Framework (the "Framework") is published on the DIFC Regulation 10 page and on the "Certification Schemes, Accreditation and Codes" register page of the DIFC website.

B) How is the certification assessed and granted? An Accredited Certification Body, which is an entity that has applied to the Commissioner for accreditation, awards and monitors certification of Certification Applicants.

C) **What is assessed?** In line with Regulation 10, the System, not the Certification Applicant, is assessed. The Certification Applicant does play a part, however, in ensuring that all necessary requirements are in place for the System to be certified.

Q12. What constitutes "commercial use of a System"?

Commercial use is similar to the concept of placing a System in the consumer market, i.e., as per the European Union Artificial Intelligence Act (Regulation (EU) 2024/1689 or the "**EU AI Act**"). There is a consumer use (and consequently, consumer protection) element to this piece of Regulation 10, hence the need for both risk assessment of a System for HRP and subsequent certification of the System. It is also why Regulation 10 links to Regulation 6.2 on unfair or deceptive practices.

Q13. Is there a fee for accreditation or certification?

Yes. Fees are determined by the Commissioner if he awards accreditation to an Applicant Accredited Certification Body ("ACB") or by the ACB that is empowered to issue accreditation or certification. Fees must be reasonable and not excessive. If a fee appears to be excessive, please contact the Commissioner or his office for support.

Please check with the relevant entity for its fees and other requirements to begin the accreditation or certification process.

Q14. What must I have in place to begin the accreditation or certification process?

It is advisable to conduct an assessment of whether the System is to be used for High Risk Processing. The DIFC website provides an HRP assessment that may help guide your decision making about the risk level of the System, however it may be necessary to seek legal advice as a first step.

Please review the preliminary questions in Parts 1 and 2 and the flow charts about the approvals process found in the Framework for initial preparation. If an ACB has been identified for certification of the System, the parties may meet to discuss the process, preliminary requirements and any terms of reference for conducting the accreditation or certification process.

Q15. What is the waiting period to re-apply if accreditation or certification is not awarded?

Entities may re-apply after one (1) year or earlier if an exception is granted.

Q16. How long is accreditation of an ACB valid?

Accreditation is valid for five (5) years, subject to monitoring and period checks for compliance, complaints or conflicts.

Q17. How long is certification of a System valid?

Certification is valid for a maximum of three (3) years, subject to monitoring and period checks for compliance, complaints or conflicts.

6. Autonomous Systems Officer (ASO)

Q18. What is the role and function of the 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.

7. Interoperability

Q19. Are the requirements that DIFC impose by way of the Regulations and Framework similar to the conformity assessments (with CE marking) imposed under the AI Act?

There is currently no specific requirement in Regulation 10 or the Framework for "CE marking" as required by the European Union Artificial Intelligence Act (Regulation (EU) 2024/1689 or the "**EU AI Act**"). However, if the EU AI Act or other EU laws or regulations are applicable to the System design and build, then CE Marking is likely required. Please seek legal advice to ensure compliance with the EU AI Act or other applicable laws and regulations, if any.

That said, the Framework aligns with the EU AI Act Article 16 and Article 43 Obligations and Conformity Assessment criteria. In other words, for Systems that will be used for High Risk Processing, the Framework effectively acts as a conformity assessment to verify and demonstrate that a standard or technical specification was applied in the design, manufacturing, installation or maintenance / updates to a system

While Regulation 10 and the Framework are more rights and redress focused, Regulation 10.2.2, which requires that detailed notice is provided, in effect addresses similar concepts pertinent to a conformity assessment (see 10.2.2(b)(v)).

Q20. Is there a "shortcut" for accreditation/ certification if proof is provided of accreditation/ certification under the EU AI Act or other applicable AI law or regulation?

Yes. Under the DIFC DP Law, Article 50(3) permits the Commissioner to issue a certification himself (if he establishes a certification scheme) and Article 50(5) requires the Commissioner to maintain a public register of all approved certification bodies and schemes.

On either basis, if the Commissioner is asked to approve a scheme that has been used by a Deployer, Operator or Provider, for example, then it effectively fast tracks approval of that certification, which will then be listed on the Commissioner's register.

A short form application must be submitted to ensure the Commissioner is made aware of the other certification and so he can review / approve it for the register. Please see the Regulation 10 page of the DIFC website for additional information including forms and templates for the purposes of Regulation 10 compliance.

Q21. Are there compliance requirements similar to those under the EU AI Act (i.e., risk assessment and mitigation methodology, datasets quality requirements, appropriate human oversight, high levels of robustness imposed from a security and accuracy perspective, etc)?

Yes, in both the Framework and the Regs. Regulation 10 and the tools that support its implementation can stand alone as a regulatory platform on which to develop Systems, or can be seen as a supplement to Systems developed elsewhere, for example, in the EU or within the context of impacting people located in the EU.

8. Next Steps: Further Developments and Use Case Testing

Use Case testing in a data protection by design "accelerator" may be undertaken. The resulting feedback and proven case studies will feed further development of Regulation 10, including the usual consultation period, and will be 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 Regulation 10, 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.