DIFC REGULATION 10 –

Accreditation and Certification Framework For Autonomous and Semi-Autonomous Systems Processing Personal Data

("Framework")

Commissioner of Data Protection

DIFC

TABLE OF CONTENTS

Introduction

Application and Interpretation

In this Framework, a reference to "the Law" is a reference to the Data Protection Law, DIFC Law No. 5 of 2020 and a reference to "the Regulations" is a reference to the DIFC Data Protection Regulations 2020.

This Framework applies to any person to whom the Law and Regulations applies.

Definitions

Defined terms are as set out in the Law or Regulations, and otherwise as set out below. Defined terms are identified throughout this Framework by the capitalisation of the initial letter of a word or phrase. Where capitalisation of the initial letter is not used, an expression has its natural meaning.

Term	Definition
Accredited Certification Body or ACB / Applicant Accredited Certification Body or Applicant ACB	refers to a body that is applying for or has applied for and been granted accreditation status by the Commissioner in accordance with Article 51 of the Law, for the governance, development and implementation of Regulation 10.3.3 of the Regulations as it applies to Systems used for High Risk Processing. An Accredited Certification Body has the ability to certify a Certification Applicant's System for use in High Risk Processing Activities, as well as revoking, suspending and reinstating that certification status.
Accredited Certification Body Application Criteria	the framework of criteria set out in Part 1 of this Framework that an Accredited Certification Body must demonstrate and adhere to in order for the Commissioner to award and maintain its accreditation.
Authorised Signatory	a person authorised to sign confirmations and to undertake commitments or requirements on behalf of any of the bodies, persons or entities referred to in this Framework.
Certification Program Requirements / Program Requirements (CPR)	the requirements set out in Part 2 of this Framework that Certification Applicants must comply with for certification of a System to be used, operated, provided, offered, or otherwise made available for commercial use, in High Risk Processing Activities, provided an Accredited Certification Body has certified compliance with such requirements.

Term	Definition
Commissioner of Data Protection / Commissioner	Supervisory authority in the DIFC that receives applications in accordance with Article 51(1) from Accredited Certification Bodies that wish to become Accredited Certification Bodies, in accordance with Article 51(6).
Confirmation Statement	a statement given by any body, person or entity pursuant to this Framework confirming that the information provided for either certification or accreditation is true and complete.
Certification Applicant or CA	means any Controller or Processor that is processing personal Data through a System for commercial purposes that qualifies as High Risk Processing Activities, that applies for certification of a System
Framework	refers to the DIFC Regulation 10 Accreditation and Certification Framework set out herein.
System	Any machine-based system operating in an autonomous or semiautonomous manner, that can: (i) Process Personal Data for human-defined purposes or purposes that the system itself defines, or both; and (ii) generate output as a result of or on the basis of such Processing. The definition of System has been adapted on the basis of the OECD guidelines and the Regulation of the European Union on harmonised 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.

Where reference is made in this Framework to a statutory provision, it is a reference to the provision as amended, and includes a reference to that provision as extended or applied by or under any other provision, unless the contrary intention appears**.**

What is the Framework?

This Framework serves to implement Articles 50 and 51 of the Law regarding the requirement under Regulation 10.3.3(a)[1] to certify Systems used in High Risk Processing Activities. The Framework sets out the following:

[1] Updated Regulations enacted on September 1, 2023, available here and updated from time to time: https://www.difc.ae/business/laws-and-regulations/legal-database/difc-laws/data-protection-law-difc-law-no-5-2020

- The application process that governs an application for becoming an Accredited Certification Body, including the specific accreditation application criteria that the Commissioner shall review when assessing such organisations; and

- Part 2: Certification for how an Accredited Certification Body certifies a Certification Applicant's System used in or for High Risk Processing Activities

Article 51 of the Law provides the Commissioner with the authority to award accreditation to Applicant Accredited Certification Bodies that will, in turn, certify Systems of entities seeking to use, operate, provide, offer, or otherwise make available for commercial use such System for High Risk Processing Activities.[2] The timeline for implementing the Framework is at the discretion of the Commissioner.

Why is the Framework necessary?

The Regulations mandate that no person may use, operate, provide, offer or otherwise make available for commercial use a System to engage in High Risk Processing Activities unless all audit and certification requirements established by the Commissioner are satisfied. As such, this Framework provides the criteria that enable compliance with Regulation 10.3.3.

Updates to the Framework

The Framework may be updated for a number of reasons, including but not limited to:

- annual reviews on the effectiveness of the Framework;
- amendments to the Law or Regulations;
- revised or more relevant examples of acceptable evidence for applications;
- alignment with global best practices in the regulation or certification of Systems; or
- technological changes relevant to the Framework that warrant an update.

Guidance and FAQs about Regulation 10 are available on the DIFC website.

Please contact the Commissioner 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.

[2] See Regulation 10.3.3

Part 1: Accreditation

Introduction

In accordance with Article 51 of the Law, the accreditation application criteria shall be adhered to for organisations seeking to become an Accredited Certification Body. An Accredited Certification Body has the authority to certify a Certification Applicant's Systems used for High Risk Processing Activities in accordance with Regulation 10.3.3.

The approval of Accredited Certification Bodies necessitates a thorough assessment by the Commissioner to confirm their compliance with the relevant criteria. Accreditation status is valid for five (5) years from the date of initial approval as an Accredited Certification Body.

The Commissioner retains the authority to conduct periodic risk-based reviews of an Accredited Certification Body to verify continued adherence to accreditation application criteria. These reviews may be initiated by amendments to the Framework, application standards, significant changes within an Accredited Certification Body's business structure or internal governance, or instances where an Accredited Certification Body fails to fulfil its prescribed functions. Applications to become an Accredited Certification Body shall be submitted in English, accompanied by the necessary documentation pertinent to the accreditation criteria, to the Commissioner for consideration.

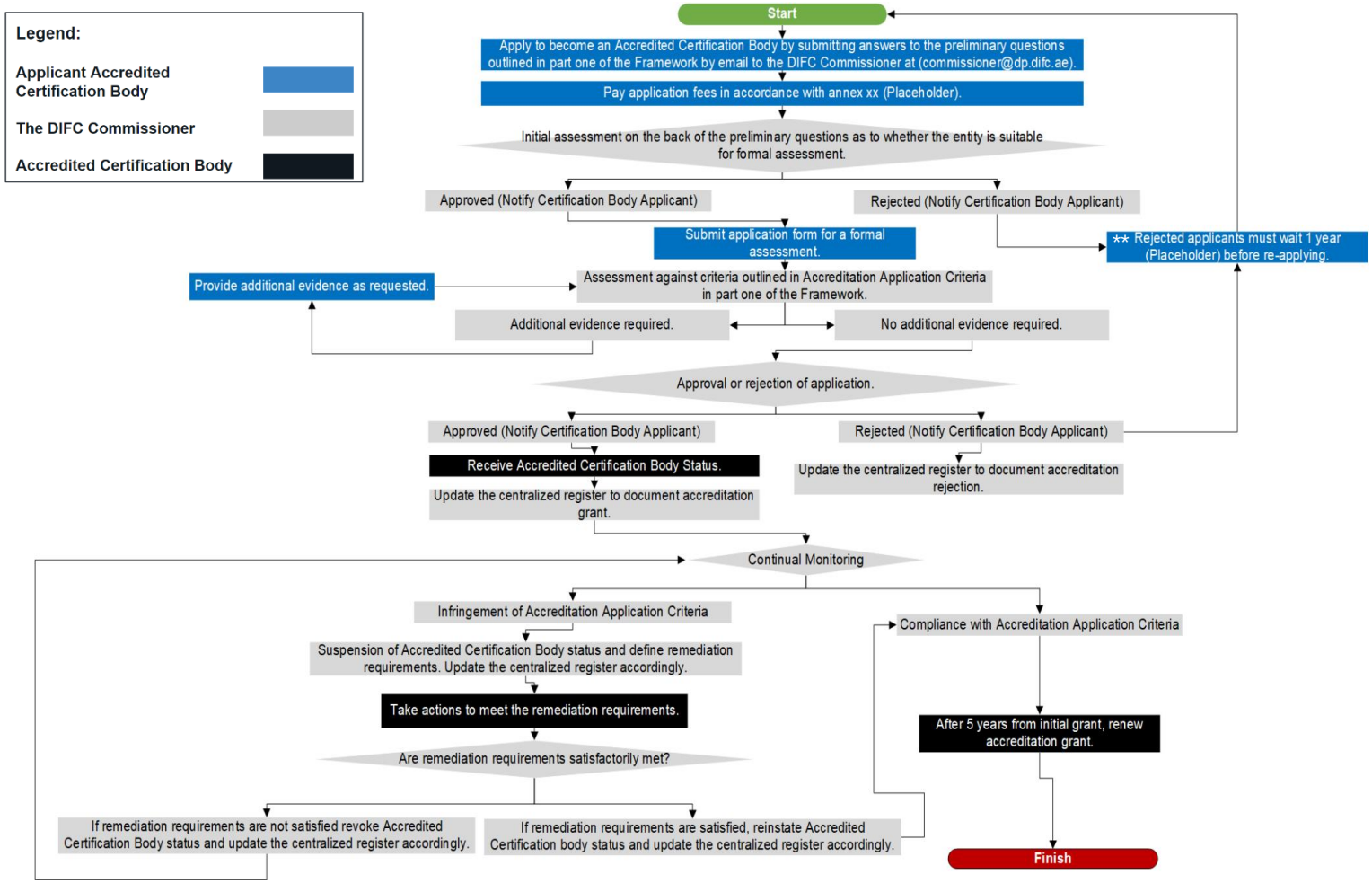
Preliminary Questions

- *Please provide the name of the Applicant Accredited Certification Body.*
- *Please provide the Applicant Accredited Certification Body's commercial license or other relevant business registration information that clearly identifies the jurisdiction authorising its commercial activities.*
- *Who is the organisation's designated point of contact?*
- *Who is the organisation's Authorised Signatory?*
- *Is the Applicant Accredited Certification Body subject to the jurisdiction of a relevant enforcement authority within its home jurisdiction, i.e., data protection or other similar supervisory authority that is empowered to take enforcement action?*
- *Will the Applicant Accredited Certification Body, once accredited, certify a System in use or intended to be used by its own organisation or within the same group of companies? (Please see additional requirements, including conflicts of interest measures, applicable in such circumstances below.)*
- *If registered in the DIFC, please provide a confirmation statement for the organisation.*

Prior to the start of the ACB Application process, it is recommended that the Applicant ACB meets with the Commissioner or his delegate(s) to review the responses to these preliminary questions and agree a provisional schedule for the application submission and review.

Figure 1 – Accredited Certification Body Application Process Flow

*** Please note that exceptions may be granted by the Commissioner or another ACB that is empowered to reassess the Applicant ACB's application.*



Accredited Certification Body Application Criteria

The Commissioner shall only approve an application to become an Accredited Certification Body where an organisation has satisfied the conditions set out in Article 51 of the Law. Evidence of each requirement shall be assessed against the supporting documents provided.

1 Independence

Explanatory Note:

An Applicant Accredited Certification Body shall be required to demonstrate its independence from a functional, financial, organisational and from an accountability-based decision-making perspective.

1.1 Requirements

An Applicant Accredited Certification Body shall demonstrate to the satisfaction of the Commissioner its independence in general and from the Commissioner or his delegate(s).

1.2 Functional:

1.2.1 An Applicant Accredited Certification Body shall provide evidence during the application process that its personnel will act independently, with the requisite skill and without undue pressure or influence. This includes demonstrating:

(a) The autonomy to make impartial decisions regarding certification without undue influence from third parties or related parties.

Examples of Acceptable Evidence

- *Assessments take place against objective standards and criteria and decisions are made solely on evidence collected during an assessment;*
- *no consideration is given to the CA's influence, reputation, business or financial relationships;*
- *Decisions can be justified with clear and transparent rationale;*
- *The ACB operates under strict policies that prevent external entities from influencing certification decisions; and*
- *There is an established and independent appeals process to contest certification decisions*

(b) Clear documented procedures that ensure independence in operational activities, especially in relation to assessment and certification processes;

(c) Possessing the competency necessary and sufficient expertise to evaluate Certification Applicants and their Systems without external pressure or influence;

(d) the objective supervision of resources and finances of an Applicant Accredited Certification Body.

Examples of Acceptable Evidence

- *A specific budget allocated to an Applicant Accredited Certification Body for the purposes of undertaking the certification process, demonstrating that Applicant Accredited Certification Body personnel act independently and are not influenced by budgetary or other commercial factors.*

(e) Decisions about, and key performance indicators (KPIs) imposed on an Applicant Accredited Certification Body or its personnel;

Examples of Acceptable Evidence

- *Any relevant (contractual or organisational) KPI policy or process may be provided.*

- *Procedures clearly setting out the functioning of internal governance including any relevant decision-making process and reporting procedures within the organisation or group of companies within the organisation. The documentation provided may also include job descriptions, management reports and policies aiming to raise personnel awareness of governance structures and relevant procedures, as well as independent audit or review of KPIs.*

and

(f) safeguarding impartiality, in terms of equal treatment of all Certification Applicants seeking certification of relevant Systems.

Examples of Acceptable Evidence

- *Documented recruitment processes ensuring that Applicant Accredited Certification Body personnel who are retained will be empowered and encouraged to act independently and without undue influence.*

- *Job descriptions outlining the requirement to act independently and safeguard impartiality when given a task that requires fair, uncompromised review of a System or the Certification Applicant requesting certification.*

- *Risk registers that identify and assess risks related to controls for potentially compromised impartiality, particularly where the Certification Applicant seeking certification is within the same Group or affiliated with an Applicant Accredited Certification Body, once accredited.*

1.2.2 If an Applicant Accredited Certification Body intends to certify a System or Systems for use or in use within its own organisation or within a group of companies in which it is an affiliate, enhanced due diligence or further evidence of independence is required. If valid independence cannot be demonstrated, an Applicant Accredited Certification Body cannot apply for accreditation status in order to certify such Systems, unless an exception is requested and approved by the Commissioner. Additional requirements are addressed in Section 6, Conflicts of Interest.

Examples of Acceptable Evidence

- *Demonstration that different directors or senior decision makers are involved in certification of the System.*

- *Any other information that the Commissioner may request.*

1.3 Financial / Material:

1.3.1 An Applicant Accredited Certification Body shall demonstrate that it has the financial stability and resources for the operation of its accreditation or certification activities, and may utilise them independently, subject to administrative approvals where necessary within the organisational policies or by applicable laws.

Examples of Acceptable Evidence

- *Certificate of insurance (professional liability) covering its monitoring tasks.*

- *Any other evidence of financial assets or financial documents demonstrating its financial stability.*

1.3.2 An Applicant Accredited Certification Body shall be able to manage its budget and resources independently and effectively monitor compliance without any form of influence.

Examples of Acceptable Evidence

- *Specific and sufficient budget allocated to an Applicant Accredited Certification Body which has enough financial resources to conduct the accreditation without compromising quality.*

1.3.3 An Applicant Accredited Certification Body shall demonstrate to the Commissioner the means by which it obtains financial support for its role as an Accredited Certification Body and explain how this does not compromise its independence.

Examples of Acceptable Evidence

- *Specific budget allocated to an Applicant Accredited Certification Body.*
- *Any other evidence of financial assets and documents demonstrating an Applicant Accredited Certification Body's financial independence.*

1.4 Organisational:

1.4.1 An Applicant Accredited Certification Body shall provide information concerning its corporate governance structures including ultimate beneficial ownership, board of directors or other corporate structure information not otherwise publicly available. If necessary, specific evidence must be provided showing vertical, independent separation of relationships with other groups or affiliated Certification Applicants who seek certification and shall evidence its impartiality.

Examples of Acceptable Evidence

- *Information barriers and controls preventing the misuse of confidential information.*
- *Separate reporting.*
- *Separate operational functions.*
- *Group ownership or line management structure and management functions, demonstrating effective organisational independence.*
- *Use of different logos or names where appropriate.*

1.4.2 An Applicant Accredited Certification Body shall demonstrate that it has adequate resources and personnel to effectively perform its tasks, as well as to compensate them appropriately.

Examples of Acceptable Evidence

- *The recruiting process of the personnel required to fulfil this role within an Applicant Accredited Certification Body, demonstrating that employees in this role possess adequate skills, and technical expertise to perform its tasks.*
- *Organisational chart, demonstrating that an Applicant Accredited Certification Body has sufficient and adequate personnel assigned and headcount to perform tasks.*
- *Documentation demonstrating appropriate compensation for this specific role, as well as the duration of tenure in said role, role description / contracts or any other formal agreement between the employee fulfilling the role and the Applicant Accredited Certification Body.*

1.4.3 Where an Applicant Accredited Certification Body engages subcontractors in relation to the provision of accreditation services either in part or in full, it shall ensure that sufficient guarantees are in place in terms of the knowledge, technical expertise, reliability, and resources of the sub-contractor. An Applicant Accredited Certification Body's obligations are also applicable to the sub-contractor. The use of sub-contractors does not remove or delegate responsibility of an Applicant Accredited Certification Body who shall remain ultimately responsible for compliance with its obligations as an Accredited Certification Body.

Examples of Acceptable Evidence

- *A clear procedure for subcontracting including the conditions under which this may take place, such as an approval process.*

- *Sufficient documented procedures to guarantee independence, expertise and other criteria as set out in this document lack conflicts of interests of the sub-contractors.*

1.4.4 Any actions taken or decisions made by an Applicant Accredited Certification Body related to its accreditation functions shall not be subject to input or approval by any other organisation.

Examples of Acceptable Evidence

- *A written statement confirming that the actions taken, or decisions made by an Applicant Accredited Certification Body are not subject to input or approval by any other organisation.*

- *Any relevant (contractual or organisational) document may be provided which demonstrates the actions taken or decisions made by an Applicant Accredited Certification Body are not subject to input or approval by any other organisation.*

1.5 Accountability:

1.5.1 An Applicant Accredited Certification Body shall provide evidence to demonstrate that it can be held accountable for its decisions and actions by any interested party, including mechanisms for complaint and appeal of decisions.

Examples of Acceptable Evidence

- *A framework for its roles and reporting procedures.*
- *Decision-making process to ensure independence.*
- *Job descriptions that evidence segregation of duties.*
- *Policies to increase awareness among the personnel about the governance structures.*
- *Procedures in place e.g., training reinforcing segregation of duties.*

- *Description of mechanisms for complaint and appeal.*

1.6 Commissioner's Acceptance Procedures for Independence Requirements

Please see Appendix B, Table 1

2 Expertise in relation to the subject-matter of the certification

Explanatory Note:

An Applicant Accredited Certification Body shall be assessed for its ability to demonstrate its expertise in accordance with this section of the criteria. Expertise requirements take into account various factors such as the specific sector of the criteria, the size of the sector, the number of committees within the sector, the risks tied to the Processing activities and the different interests at stake.

Requirements:

An Applicant Accredited Certification Body shall demonstrate to the satisfaction of the Commissioner its expertise in relation to the subject matter of the certification, in this case, the safe and ethical use of autonomous or semi-autonomous systems for use in High Risk Processing Activities itself. Detailed criteria are outlined below.

2.1 An Applicant Accredited Certification Body shall demonstrate that it has an in-depth understanding, knowledge, and experience regarding the risks and impact of High Risk Processing activities on Data Subjects, as well as governance and controls best practices applied to High Risk Processing activities.

Examples of Acceptable Evidence

- *Status as a recognised and traceable professional standards body or with qualifications from such a body.*
- *Publications and research regarding Processing activities, including High Risk Processing activities.*
- *Case studies or success stories regarding Processing activities.*
- *Recruitment process taking into account specific knowledge and experience, including High Risk Processing activities.*
- *Biographies, resumes, or curricula vitae of key staff attesting to their possessing relevant expertise.*

2.2 Subject to the Commissioner's discretion, an Applicant Accredited Certification Body and the personnel performing certification assessments shall demonstrate experience in autonomous and semi-autonomous Systems design, along with technical and organisational understanding and awareness of related emerging technology, more specifically around the promulgation and use of Systems used for, directly or indirectly, Processing Personal Data, e.g., generative AI and machine learning-based Systems, particularly when used for High Risk Processing activities.

Examples of Acceptable Evidence

- *Research and publications regarding qualification, installation, deployment or development of Systems.*
- *Training and certifications (if available) related to qualification, installation, deployment or development of Systems.*
- *Case studies involving Systems.*
- *Recruitment process taking into account specific knowledge and experience.*

2.3 An Applicant Accredited Certification Body shall demonstrate that it employs staff that have the necessary legal or compliance expertise to conduct comprehensive risk assessments and to assess the impact on the availability of rights and redress for Data Subjects.

Examples of Acceptable Evidence

- *Job description template specifying legal and compliance skills.*
- *Hiring or assignment process including this requirement.*
- *Training programs relating to legal and compliance expertise vis a vis conducting risk assessments or developing assessment methodologies.*
- *Certifications of staff related to legal and compliance expertise*
- *Certification of staff demonstrating proven experience of conducting audits and assessments, specifically with respect to privacy and security*

2.4 An Applicant Accredited Certification Body shall demonstrate that it has an understanding of the evolution of the Law, the Regulations, and other applicable regulations, practices, and standards regarding Personal Data, or, where applicable, of Systems.

Examples of Acceptable Evidence

- *Job description template specifying knowledge of the applicable data protection regulations.*
- *Hiring or assignment process including this requirement.*
- *Research and publications related to the applicable data protection regulations.*

2.5 An Applicant Accredited Certification Body shall demonstrate that it has experience liaising with data protection regulators, technology regulators, or government authorities.

Examples of Acceptable Evidence

- *Documentation of past engagements with data protection regulators, technology regulators, or government authorities.*

- *References and testimonials from data protection regulators, technology regulators, or government authorities.*
- *Participation in regulatory forums.*
- *Compliance reports and audits.*
- *Legal proceedings or investigations.*
- *Policy advocacy and engagement.*

2.6 An Applicant Accredited Certification Body shall be sufficiently resourced, and personnel shall demonstrate sufficient knowledge and experience in handling complaints.

Examples of Acceptable Evidence

- *Job description template specifying knowledge and experience in complaints handling.*
- *Training programs or certifications related to handling complaints.*

2.7 An Applicant Accredited Certification Body shall ensure that it meets any additional requirements or standards set by the Commissioner for accreditation, as communicated through official channels.

Examples of Acceptable Evidence

- *Produce any document justifying the implemented measures to meet this requirement. e.g. updated policies reflecting alignment with accreditation criteria.*

2.8 Commissioner's Acceptance Procedures for Expertise Requirements

Please see Appendix B, Table 2

3 Written Undertakings

Explanatory Note:

An Applicant Accredited Certification Body shall be assessed on its commitment to adhere to the relevant Certification Program Requirements and to and applicable laws.

Requirements:

3.1 An Applicant Accredited Certification Body shall formally commit in writing to adhere to the criteria of the relevant certification scheme it applies to a System assessment, on a case-by-case basis, and to respect the criteria of the proposed scheme. It must also confirm that it in completing the assessment as well as in applying the assessment criteria, it will comply with applicable laws, including intellectual property laws governing the use of relevant marks regarding certification, if any.

Examples of Acceptable Evidence

- *A formal agreement or a Memorandum of Understanding (MoU) between an Applicant Accredited Certification Body and the DIFC Commissioner specifying an Applicant Accredited Certification Body's commitment to the criteria of the certification scheme.*

3.2 Commissioner's Acceptance Procedures for Written Undertaken Requirements

Please see Appendix B, Table 3

4 Established procedures

Explanatory Note:

An Applicant Accredited Certification Body shall be assessed on established procedures for the issuing, periodic review / re-certification, and withdrawal of certification, enforcement of certification requirements, and use of seals, and marks in connection with the proposed certification scheme. It must demonstrate whether the monitoring tasks and duties it carries out are regular, timely and complete. The monitoring procedures implemented by an Applicant Accredited Certification Body shall be in accordance with this framework.

Requirements:

4.1 An Applicant Accredited Certification Body shall demonstrate that it has a relevant procedure to check the eligibility of Certification Applicants to apply for certification of its System and maturity or experience of its staff, its ability to comply with criteria and subsequently the issuance or withdrawal of the certification awarded.

Examples of Acceptable Evidence

- *Documentation verification processes for assessing the authenticity and accuracy of documents provided by Certification Applicants.*
- *On-site or other relevant audit procedures to inspect the eligibility of Certification Applicants.*
- *Compliance assessment procedure documentation.*

4.2 An Applicant Accredited Certification Body shall demonstrate that it has a procedure to require proof that the Certification Applicant or their Directors, IT developers or other relevant staff involved in the use, operation, offer or commercial availability of its Systems are not the subject of any investigations or regulatory action that might prevent certification from being issued.

Examples of Acceptable Evidence

- *Procedures for background checks for relevant staff of the Certification Applicant.*
- *Procedures for disclosure, mandating Certification Applicants to disclose any ongoing investigations or regulatory actions.*
- *Procedures for documentation review verifying Certification Applicants' legal status.*

4.3 An Applicant Accredited Certification Body shall demonstrate that its audit or review procedures define technical and governance requirements for applying appropriate safeguards and controls to the relevant Systems, the type of assessment, where applicable, and a procedure to document the findings.

Examples of Acceptable Evidence

Audit or Review procedures can include:

- *Audit methodology with the defined requirements for assessing High Risk Processing through System's*
- *Self-assessment reports or questionnaires with the defined requirements.*

4.4 An Applicant Accredited Certification Body shall demonstrate that it has a procedure and decision making process for determining when to conduct periodic compliance assessments and continual monitoring of Certification Applicants with certified Systems, taking into account criteria such as the complexity of Personal Data Processing and data protection related autonomous or semi-autonomous processing risks involved, geographical and data protection jurisdictional scope and influencing factors, and any current relevant recent investigation/regulatory action.

Examples of Acceptable Evidence

- *Compliance assessment procedure documentation.*
- *Assessment reports.*
- *Risk assessment documentation.*
- *Complaint handling records.*

4.5 An Applicant Accredited Certification Body will require Certification Applicants to attest on [an annual basis] to the continuing adherence to the Systems Certification Program Requirements. Regular comprehensive reviews will be carried out to ensure the integrity of the re-Certification.

4.5.1 Where there has been a material change within the certified Systems or the Certification Applicants' structure, policies or processes (as self-reported by the Applicant or as reasonably determined by an Accredited Certification Body in good faith), an immediate review process will be carried out in accordance with the process set out in Section 8.2.

4.5.2 Where an Applicant Accredited Certification Body, once accredited, verifies that necessary changes, if any, have been made and that re-certification is warranted, it shall provide notice as to whether the System is in compliance with the relevant Certification Program Requirements and that it has been re-certified.

4.6 An Applicant Accredited Certification Body shall demonstrate that it has a procedure for the investigation, identification and management of a Certification Applicant's certified System infringements regarding ongoing compliance with the Certification Program Requirements and additional controls to ensure appropriate action is taken to remedy such infringements as set out in the relevant criteria.

Examples of Acceptable Evidence

- *Investigation procedure documentation.*
- *Management protocol for decision making regarding investigation findings.*
- *Procedures to take appropriate remedial actions.*
- *Procedures for documentation of actions taken by a Certification Applicant in attempts to reinstate certification status for its System.*

4.7 An Applicant Accredited Certification Body must demonstrate that it shall be responsible for the management of all information obtained or created during the application and certification process. An Applicant Accredited Certification Body shall ensure that relevant personnel keep all information obtained or created during the performance of certification process tasks confidential, unless they are required to disclose or are exempt from a duty of confidentiality by law.

Examples of Acceptable Evidence

- *Relevant confidentiality / Data Protection policy, notification, compliance program information*
- *Training in confidentiality and handling of information.*
- *Access controls to repositories containing information relevant to the application and certification process.*

4.8 Applicant Accredited Certification Body must demonstrate that it has the authority to enforce its program requirements against Certification Applicants, either through contract or by law.

4.8.1 Accredited Certification Body must demonstrate that it will refer a matter to the appropriate public authority or enforcement agency for review and possible enforcement action, where an Accredited Certification Body has a reasonable belief pursuant to its established review process that a Certification Applicant's failure to comply with the certification scheme requirements has not been remedied within a reasonable time under the procedures established by an Accredited Certification Body, so long as such failure to comply can be reasonably believed to be a violation of applicable law.

4.8.2 Where possible, an Accredited Certification Body must demonstrate that it will respond to requests from relevant enforcement entities that reasonably relate to the certification application review-related activities of an Accredited Certification Body.

Examples of Acceptable Evidence

- *process in place for notifying Participant immediately of non-compliance with Accredited Certification Body's program requirements and for requiring Participant to remedy the non-compliance within a specified time period.*

- *processes in place to impose the following penalties, which is proportional to the harm or potential harm resulting from the violation, in cases where a Participant has not complied with the program requirements and has failed to remedy the non-compliance within a specified time period. [NOTE: In addition to the penalties listed below, Accredited Certification Body may execute contracts related to legal rights and, where applicable, those related intellectual property rights enforceable in a Court of law.]*

  a) *Requiring Participant to remedy the non-compliance within a specified time period, failing which an Accredited Certification Body shall remove the Participant from its program.*

  b) *Temporarily suspending the Certification Applicant's right to display an Accredited Certification Body's seal.*

  c) *Naming the Participant and publicising the non-compliance.*

  d) *Referring the violation to the relevant public authority or privacy enforcement authority. [NOTE: this should be reserved for circumstances where a violation raises to the level of a violation of applicable law.]*

  e) *Other penalties – including monetary penalties – as deemed appropriate by an Accredited Certification Body and as recommended to the Commissioner.*

4.9 Commissioner's Acceptance Procedures for Established Procedures requirements

Please see Appendix B, Table 4

5 Transparency, complaints handling and dispute resolution

Explanatory Note:

An Applicant Accredited Certification Body shall be assessed on the procedures implemented to process complaints and appeals regarding infringements of the certification of a Certification Applicant's certified System or the manner in which the certification has been or is being implemented. The Certification Body Application must demonstrate that it will make those procedures and structures transparent to Data Subjects and the public.

Requirements:

5.1 Managing complaints about infringements of the certification of a Certification Applicant's System

5.1.1 An Applicant Accredited Certification Body must demonstrate that it shall provide evidence of a procedure to handle complaints about a Certification Applicant's certified System or from any Data Subject whose Personal Data is processed by a System. This process for complaints handling and decision-making shall be publicly available, accessible and easily understood.

Examples of Acceptable Evidence

- *Template of complaints handling procedure (including contact details, how the complaint is presented, how the complaint is followed-up on, how the complainant is informed, the consequences shall the complaint be rejected, the consequences shall the complaint be considered justified, etc.)*

- *Standard contact form and/or screenshot of contact details from an Applicant Accredited Certification Body's website.*

5.1.2 An Applicant Accredited Certification Body must demonstrate that it shall acknowledge receipt of the complaint and provide the complainant with a progress report or the final decision of the investigation within a reasonable time, such as one month.

Examples of Acceptable Evidence

- *Template of acknowledgment of receipt of complaints, response template, etc. Every decision taken shall be reasonably justified and explained as transparently as possible to the complainant.*

5.1.3 An Applicant Accredited Certification Body must demonstrate that it shall maintain a record of all complaints and actions that the Commissioner can access at any time, and

that is has a policy for reporting the same to the Commissioner or other relevant party at least bi-annually or as needed, based on case-by-case circumstances.

Examples of Acceptable Evidence

- *Template of sheet recording complaints received and processed and related statistics. This record includes the nature of the complaint, the identity of the concerned Entity and of the complainant, the forms and delays of complaints handling and the reason for closing the complaint.*

5.1.4 An Applicant Accredited Certification Body must demonstrate that it shall have the necessary measures in place to manage cases of infringement by a Certification Applicant's certified System of the certification criteria, and where applicable, to stop the infringement and avoid future recurrence. Such measures shall include identifying infringement of criteria, issuing remediation requirements, documenting the incident and actions taken to resolve it, notifying the DIFC Commissioner, and actioning potential suspensions or revocations of certification status.

Examples of Acceptable Evidence

- *Any relevant procedure or process to manage infringements of the certification criteria.*

5.1.5 An Applicant Accredited Certification Body must demonstrate that it shall maintain a record of all complaints and actions which the Commissioner can access at any time.

Examples of Acceptable Evidence

- *Template of sheet recording complaints received and processed. This record should include the nature of the complaint, the identity of the concerned Entity and of the complainant, the relevant forms for and record of any potential delays in complaints handling and the reason for closing the complaint.*

5.1.6 An Applicant Accredited Certification Body must demonstrate that decisions shall be accessible and easily understood, as well as made publicly available in line with its relevant complaints handling procedure. This information could include but is not limited to, general statistical information concerning the number and type of complaints/infringements, and the resolutions/appropriate actions issued and shall include information concerning any action leading to suspensions or revocations of certification status.

Examples of Acceptable Evidence

- *Template of sheet recording complaints received and processed. This record shall demonstrate the output of complaints and the complaint resolution.*

5.1.7 An Applicant Accredited Certification Body must demonstrate that it shall assist in and comply with the Commissioner's investigation into and resolution of any complaints about a Certification Applicant's certified System.

Examples of Acceptable Evidence

- *Template of complaints handling procedure (including contact details, how the complaint is presented, how the complaint is followed-up on, etc.) This procedure must specify, e.g. how the complainant is informed, the outcomes, should the complaint be rejected, or the outcomes should the complaint be considered justified.*

5.2 **Management of complaints and appeals about how the certification has been or is being implemented by a relevant Controller or Processor**

5.2.1 An Applicant Accredited Certification Body must demonstrate that it shall provide evidence of a clear procedure for a publicly available, accessible, and easily understood complaints handling and decision-making process in relation to complaints made against it.

Examples of Acceptable Evidence

- *Template of complaints handling procedure (including contact details, how the complaint is presented, how the complaint is followed-up on, how the complainant is informed, the consequences shall the complaint be rejected, the consequences shall the complaint be considered justified, etc.)*

- *Standard contact form and/or screenshot of contact details from an Applicant Accredited Certification Body's website.*

- *A process for receiving complaints and determining whether a complaint concerns the Certification Applicant's obligations and that the filed complaint falls within the scope of the certification programs requirements.*

5.2.2 An Applicant Accredited Certification Body must demonstrate that it has a documented appeals process which shall be made publicly available, accessible and easily understood and transparent. The process shall be non-contentious and shall specify that any relevant party affected by an outcome of the complaints handling process may appeal it within (thirty) 30 days.

Examples of Acceptable Evidence

- *Template of complaints handling procedure (including contact details, how the complaint is presented, how the complaint is followed-up on, etc.) This procedure specifies, e.g., how the complainant is informed, the consequences should the complaint be rejected, or the consequences should the complaint be considered justified.*

- *Standard contact form and/or screenshot of Applicant Accredited Certification Body website.*

5.2.3 The handling process for appeals shall include at least the following:

(a) a description of the process for receiving, validating, investigating the appeal and deciding what actions are to be taken in response to it;

Examples of Acceptable Evidence

- *Template of complaints handling procedure (including contact details, how the complaint is presented, how the complaint is followed-up on, etc.) This procedure specifies, e.g. how the complainant is informed, the consequences should the complaint be rejected, or the consequences should the complaint be considered justified.*

(b) tracking and recording appeals, including actions undertaken to resolve them; and

Examples of Acceptable Evidence

- *Template of sheet recording complaints received and processed. This record includes the nature of the complaint, the identity of the concerned criteria Body and of the complainant, the relevant forms for and record of any delays in complaints handling and the reason for closing the complaint.*

(c) ensuring that any appropriate action is taken in a timely manner.

Examples of Acceptable Evidence

- *Template of acknowledgment of receipt of complaints, response template, etc. Every decision shall be justified.*

5.2.4 An Applicant Accredited Certification Body must demonstrate that it has processed to acknowledge receipt of the appeal and provide progress reports and the final decision to the relevant party within a reasonable time, such as one month.

Examples of Acceptable Evidence

- *Template of acknowledgment of receipt of complaints, response template, etc. Every decision shall be justified.*

5.2.5 An Applicant Accredited Certification Body must demonstrate that it has processes to assist in and comply with the investigation and resolution of any complaints about it to the Commissioner.

Examples of Acceptable Evidence

- *Template of complaints handling procedure (including contact details, how the complaint is presented, how the complaint is followed-up on, how the complainant is informed, the consequences shall the complaint be rejected, the consequences shall the complaint be considered justified, etc.*

5.3 **Dispute Resolution**

5.3.1 An Applicant Accredited Certification Body must demonstrate that it has a mechanism to resolve disputes between complainants and Certification Applicants in relation to non-compliance with its program requirements, as well as a mechanism for cooperation on dispute resolution with other Accredited Certification Bodies recognised by the Commissioner when appropriate and where possible. An Applicant Accredited Certification Body may choose not to directly supply the dispute resolution mechanism.

5.3.2 The dispute resolution mechanism may be contracted out by an Applicant Accredited Certification Body to a third party to supply a dispute resolution service. Where the dispute resolution mechanism is contracted out by Applicant Accredited Certification Body, the relationship must be in place at the time an Applicant Accredited Certification Body is accredited.

Examples of Acceptable Evidence:

- *A confidential and timely process for resolving complaints. Where non-compliance with any of the program requirements is found, an Accredited Certification Body (or contracted third party supplier of a dispute resolution service) will notify the Certification Applicant outlining the corrections that need to be made and the reasonable timeframe within which the corrections must be completed.*

- *Written notice of complaint resolution by an Accredited Certification Body or contracted third party supplier of the dispute resolution service to the complainant and the Participant.*

- *Where relevant, a process for obtaining an individual's consent before sharing that individual's personal information with the relevant enforcement authority in connection with a request for assistance.*

- *A process for making publicly available the statistics on the types of complaints received by an Accredited Certification Body or contracted third party supplier of a dispute resolution service and the outcomes of such complaints, and for communicating that information to the relevant government agency and privacy enforcement authority (see Annex A for sample template)*

- *A process for releasing in anonymised form, case notes on a selection of resolved complaints illustrating typical or significant interpretations and notable outcomes (see Annex A for sample template)*

5.4 Commissioner's Acceptance Procedures for Complaints / Dispute Resolution criteria

Please see Appendix B, Table 5

6 Absence of conflicts of interest

Explanatory Note:

An Applicant Accredited Certification Body must be free of actual or potential conflicts of interest in order to participate in the Regulation 10 Accreditation and Certification Framework. For the purposes of participation as an Accredited Certification Body, this means the ability of an Accredited Certification Body to perform all tasks related to a Certification Applicant's certification free from influences that would compromise an Accredited Certification Body's professional judgment, objectivity and integrity.

6.1 An Applicant Accredited Certification Body's personnel shall comply with all requirements set out in herein and shall report to the relevant, authorised person or persons, including but not limited to the Commissioner or other designated application reviewer, where required, any situation likely to create a conflict of interest.

6.1.1 For the avoidance of doubt, at no time may an Accredited Certification Body, as an applicant or once accredited, have a direct or indirect affiliation with any Certification Applicant that would prejudice its ability to render a fair decision with respect to the certification, including but not limited to during the application review and initial certification process; during ongoing monitoring and compliance review; during re-certification and annual attestation; and during dispute resolution and enforcement of the Regulation 10 Certification Requirements against a Certification Applicant.

6.1.2 Such affiliations, which include but are not limited to the Certification Applicant and an Accredited Certification Body, as an applicant or once accredited, being under common control such that the Certification Applicant can exert undue influence on the Accredited Certification Body, as an applicant or once accredited, constitute relationships that require withdrawal under 6.1.3(i) to (iii)

6.1.3 For other types of affiliations that may be cured by the existence of structural safeguards or other procedures, the existence of any such affiliations between an Accredited Certification Body as an applicant or once accredited and the Certification Applicant must be disclosed promptly to the Commissioner or his designated application reviewer, together with an explanation of the safeguards in place to ensure that such affiliations do not compromise the ability of an Accredited Certification Body as an applicant or once accredited to render a fair decision with respect to such an Certification Applicant. Such affiliations include but are not limited to:

(a) officers of the Certification Applicant serving on the Board of Directors of an Accredited Certification Body whether as an applicant or once in a voting capacity, and vice versa;

(b) significant monetary arrangements or commercial relationship between an Accredited Certification Body and the Certification Applicant, outside of the fee charged for certification; or

(c) all other affiliations which might allow the Certification Applicant to exert undue influence on an Accredited Certification Body regarding the Certification Applicant's certification.

Examples of Acceptable Evidence

- *Specific internal procedure for reporting a conflict of interest regarding the ability of an Accredited Certification Body as an applicant or once accredited to certify a Certification Applicant's System independently and fairly.*

- *Templates enabling personnel, including subcontractor's personnel where relevant, to report a conflict of interest.*

6.2 An Applicant Accredited Certification Body must provide evidence that internal structural and procedural safeguards are in place to address potential and actual conflicts of interest. Specifically, the Applicant Accredited Certification Body must provide evidence of a conflict of interest policy for directors, management and staff to ensure fair and impartial delivery of certification assessments, reports, complaints handling and dispute resolution.

Examples of Acceptable Evidence

- *Written policies for disclosure of potential or actual conflicts of interest and, where appropriate, withdrawal of an Accredited Certification Body from particular engagements that create conflicts. Such withdrawal will be required in cases where an Accredited Certification Body as an applicant or once accredited is related to the Certification Applicants to the extent that it would give rise to a risk that its professional judgment, integrity, or objectivity could be influenced by the relationship.*

- *Written policies governing the separation of personnel handling privacy certification functions from personnel handling sales and consulting functions.*

- *Written policies for internal review of potential conflicts of interest with Certification Applicants.*

- *Written policies for internal review and management of potential conflicts of interest within the Accredited Certification Body.*

- *Published certification standards for Certification Applicants.*

- *Mechanisms for regular reporting to the relevant government agency or public authority on certification of new Certification Applicants, audits of existing Certified Systems, and dispute resolution.*

- *Mechanisms for mandatory publication of case reports in certain, limited circumstances.*

6.3 An Applicant Accredited Certification Body, must provide evidence that it will regularly, and in any case at least annually, conduct and document conflicts of interest checks to ensure that associations for the provision of services to other Certification Bodies, or those with sub-contractual agreements from other Certification Bodies, or regarding the Certification Applicant whose Systems are being certified by an Accredited Certification Body, would not adversely affect its objective judgment vis a vis the process of reviewing Certification Applicants

Examples of Acceptable Evidence

- *Procedure or processes in place to assess and verify independence regarding Accredited Certification Bodies or any sub-contractors used by them, or regarding the Certification Applicant whose System is being certified.*

- *A written statement confirming that an Accredited Certification Body, will not provide or is not providing services to a Certification Applicant being certified by the Accredited Certification Body, nor that it has sub-contractors which are currently Accredited Certification Bodies that may inappropriately influence the outcome of a Certification Applicants application.*

6.4 An Accredited Certification Body may be engaged to perform consulting or technical services for a Certification Applicant other than services relating to their certification. Where this occurs, an Accredited Certification Body will disclose Examples of Acceptable Evidence to the Commissioner or a review that he delegates this function to (the "Designated Application Reviewer") regarding performance of such services.

Examples of Acceptable Evidence

- *The existence of the engagement; and*

- *An explanation of the safeguards in place to ensure that an Applicant Accredited Certification Body remains free of actual or potential conflicts of interest arising from the engagement[3].*

6.5 Provision of services as required herein shall not be considered performing consulting services that might trigger a prohibition contained herein.

[3] *Such safeguards may include segregating the personnel providing the consulting or technical services from the personnel performing the certification process functions described in Part 2 of this document*

6.6 Commissioner's Acceptance Procedures for Conflicts of Interests requirements

Please see Appendix B, Table 6

7 Communications with the Commissioner

Explanatory Note:

An Applicant Accredited Certification Body shall be assessed on whether it can provide information outlined in this section of the criteria regarding communications and reporting to the DIFC Commissioner on a regular basis about status of certified bodies and acceptable certification program requirements for updates to the register required by Article 50(5).

Requirements:

7.1 An Applicant Accredited Certification Body shall provide evidence of a clear mechanism that governs reporting any suspensions or revocations of a Certification Applicant's certified System to the Commissioner. This reporting framework shall require as a minimum that an Applicant Accredited Certification Body can demonstrate that it shall:

(a) inform the Commissioner promptly and in any case no later than thirty (30) days and in writing of any suspension or revocation of a Certification Applicant's System certification providing valid reasons for the decision.

Examples of Acceptable Evidence

- *Documented reporting procedure or framework.*
- *Notification records.*

(b) provide information outlining details of the suspension or revocation and actions taken; and

Examples of Acceptable Evidence

- *Documented reporting procedure or framework.*
- *Notification records.*

(c) provide evidence of actions demonstrating adherence to the suspensions or revocations of the certification status process outlined in figure 2.

Examples of Acceptable Evidence

- *Documented reporting procedure or framework.*
- *Notification records.*

7.2 An Applicant Accredited Certification Body shall provide evidence that it has a documented procedure for reinstating certification of a Certification Applicant's System

and notifying that Certification Applicant and the Commissioner of the outcome of the review or investigation.

Examples of Acceptable Evidence

- *Appeals management procedure.*
- *Notice template indicating Entities rights.*

7.3 An Applicant Accredited Certification Body shall provide evidence that it is able to record any other substantial changes (see illustrative list below) and report them to the Commissioner immediately.

Examples of Acceptable Evidence

- *Substantial changes may include, but are not limited to:*
    - *legal, financial, commercial, ownership or organisational status and key personnel; and/or*
    - *resources such as those set out in Section 1 or 2 above; or*
    - *any changes to a Certification Applicant's organisational structure or the use or design of its certified System.*

- *Any relevant document evidencing these changes would be sufficient to meet this requirement.*

7.4 Commissioner's Acceptance Procedures for Communicating with the Commissioner processes

Please see Appendix B, Table 7

8 Certification Application Review processes

Explanatory Note:

An Applicant Accredited Certification Body shall be assessed on its certification application preliminary review criteria (i.e., go or no-go requirements to promote complete applications and reduce rejections), its acceptance process to ensure consistency with relevant program requirements during the application process, and its ongoing monitoring and compliance review processes once certification has been awarded to a Certification Applicant.

8.1 An Applicant Accredited Certification Body must have a comprehensive process to review a Certification Applicant's policies and practices with respect to its compliance with Regulation 10 and the Law, and to verify its compliance with the Accredited Certification Body's Certification Program Requirements (the "Certification Review Process").

8.2 The Certification Review Process must include:

8.2.1 An initial assessment, which will include verifying the contents of relevant self-assessment forms, if any, completed by the Certification Applicant against the Certification Program Requirements applied by the Accredited Certification Body, and which may also include in-person or phone interviews or inspections of any relevant Systems and related support systems or IT architecture. The initial assessment process must provide for actions including but not limited to:

8.2.1.1 Initial assessment gap identification registers and report shared with the Certification Applicant management team; and

8.2.1.2 A maximum window for remediation, if necessary, to be completed within twelve (12) months of the initial assessment. During this time, the applicant can remediate, and then continue with the assessment without having to start afresh.

8.2.2 A comprehensive report to the Certification Applicant outlining the Accredited Certification Body's findings regarding the Certification Applicant's level of compliance with the applicable program requirements. Where non-fulfilment of any of the program requirements is found, the report must include a list of changes the Certification Applicant needs to complete for the purpose of obtaining certification.

8.2.3 Verification that any changes required under subsection 8.2.2 have been properly completed by the Certification Applicant.

8.2.4 Certification that the Certification Applicant is in compliance with the Accredited Certification Body's Certification Program Requirements.

8.3 Applicant Accredited Certification Body must provide evidence of comprehensive written procedures designed to ensure the integrity of the certification application process or where relevant the Certification Review Process, and to monitor the Certification Applicant throughout the overall certification period to ensure compliance with an Accredited Certification Body's program.

8.3.1 Where there are reasonable grounds during the certification period or upon re-certification for an Accredited Certification Body to believe a Certification Applicant or Certification Re-Applicant's practices are not aligned or are no longer aligned with the Certification Program Requirements, an enhanced review process will be immediately triggered.

8.3.2 Where non-compliance with any of the Certification Program Requirements is found, an Accredited Certification Body will notify the Certification Applicant or Certification Re-Applicant outlining the corrections that need to make and a reasonable timeframe within which the corrections must be completed. An Accredited Certification Body must verify that the required changes have been properly completed within the stated timeframe.

8.4 Commissioner's Acceptance Procedures for Certification Application Review Process requirements

Please see Appendix B, Table 8

9 Certification Program Requirements Review Mechanisms

Explanatory Note:

An Applicant Accredited Certification Body, once it is awarded accreditation and becomes and Accredited Certification Body shall be periodically assessed by the Commissioner or his delegate on whether it actively participates in any further development or extension of the Certification Program Requirements' scope and/or its content, i.e., for the purposes of continuous improvement based on current technology developments, regulation or best practices.

Requirements:

9.1 An Accredited Certification Body, once accredited, shall contribute to reviews of the overall Framework, or of the Certification Program Requirements, as needed or upon request of the Commissioner. It shall therefore ensure that upon application for accreditation, it can demonstrate that it has documented plans and procedures to conduct regular reviews to ensure that both Certification Program Requirements and this Framework (where feedback is requested) remain relevant to certifying Systems and that entities with a certified System continue to meet requirements of DIFC Regulation 10 as updated from time to time.

Examples of Acceptable Evidence

- *The Accredited Certification Body shall maintain a process for sharing information about any necessary updates to the Certification Program Requirements or this Framework*

9.2 Notwithstanding Section 9.1, an Accredited Certification Body, once accredited, shall provide the Commissioner and any other relevant establishment or institution with an annual report on the operation of the Certification Program Requirements. The annual report shall include evidence regarding sub-points (a) through (e) below:

(a) information concerning any newly certified Systems and whether any gaps were revealed or revision to the Certification Program Requirements or Framework should be made;

Examples of Acceptable Evidence

- *No examples required at this time.*

(b) details of any suspensions and exclusions of any Certification Applicants' Systems;

Examples of Acceptable Evidence

- *No examples required at this time.*

(c) confirmation that a review of the Accredited Certification Body's Certification Program Requirements has taken place and the outcome of that review;

Examples of Acceptable Evidence

- *No examples required at this time.*

(d) that there are no substantial organisational or other relevant material changes to an Accredited Certification Body or its relevant certification processes; and

Examples of Acceptable Evidence

- *No examples required at this time.*

(e) information concerning Personal Data breaches vis a vis a Certification Applicant's certified System, or complaints made against the System or Accredited Certification Body.

Examples of Acceptable Evidence

- *No examples required at this time.*

9.3 An Accredited Certification Body shall apply relevant updates and implement amendments and extensions to the Certification Program Requirements as instructed by relevant stakeholders (if any) or the Commissioner.

Examples of Acceptable Evidence

- *No examples required at this time.*

9.4 An Accredited Certification Body shall ensure that information concerning its functions is recorded and made available to the Commissioner as required.

Examples of Acceptable Evidence

- *No examples required at this time.*

9.5 Commissioner's Acceptance Procedures for Certification Application Review Process requirements

Please see Appendix B, Table 9

Part 2: Certification

Introduction

The Systems certification criteria apply to any Certification Applicant that seeks certification for a System engaging in High Risk Processing Activities under the Law and Regulation 10, specifically Regulation 10.3.3.

The certification of a System for High Risk Processing Activities necessitates a thorough assessment by an Accredited Certification Body including audit criteria, or, in exceptional circumstances, the Commissioner to confirm fulfilment of the certification criteria. Such exceptional circumstances may result from the absence or unavailability of an Accredited Certification Body at the given time of application. The certification is valid for three (3) years from the date of initial certification.

The Commissioner retains the authority to conduct periodic risk-based reviews of a Certification Applicant's certified System to verify continued adherence to the certification criteria. These reviews may be initiated by amendments to the certification criteria, significant changes to the Certification Applicant's certified System that warrant a reassessment, recurring, verified complaints about use of the System that negatively impacts Data Subjects, or instances where the Certification Applicant's certified System fails to adhere to the conditions of certification.

Applications to certify a Certification Applicant's System shall be submitted in English, accompanied by documentation pertinent to the certification criteria, to an Accredited Certification Body, or in exceptional circumstances, the Commissioner.

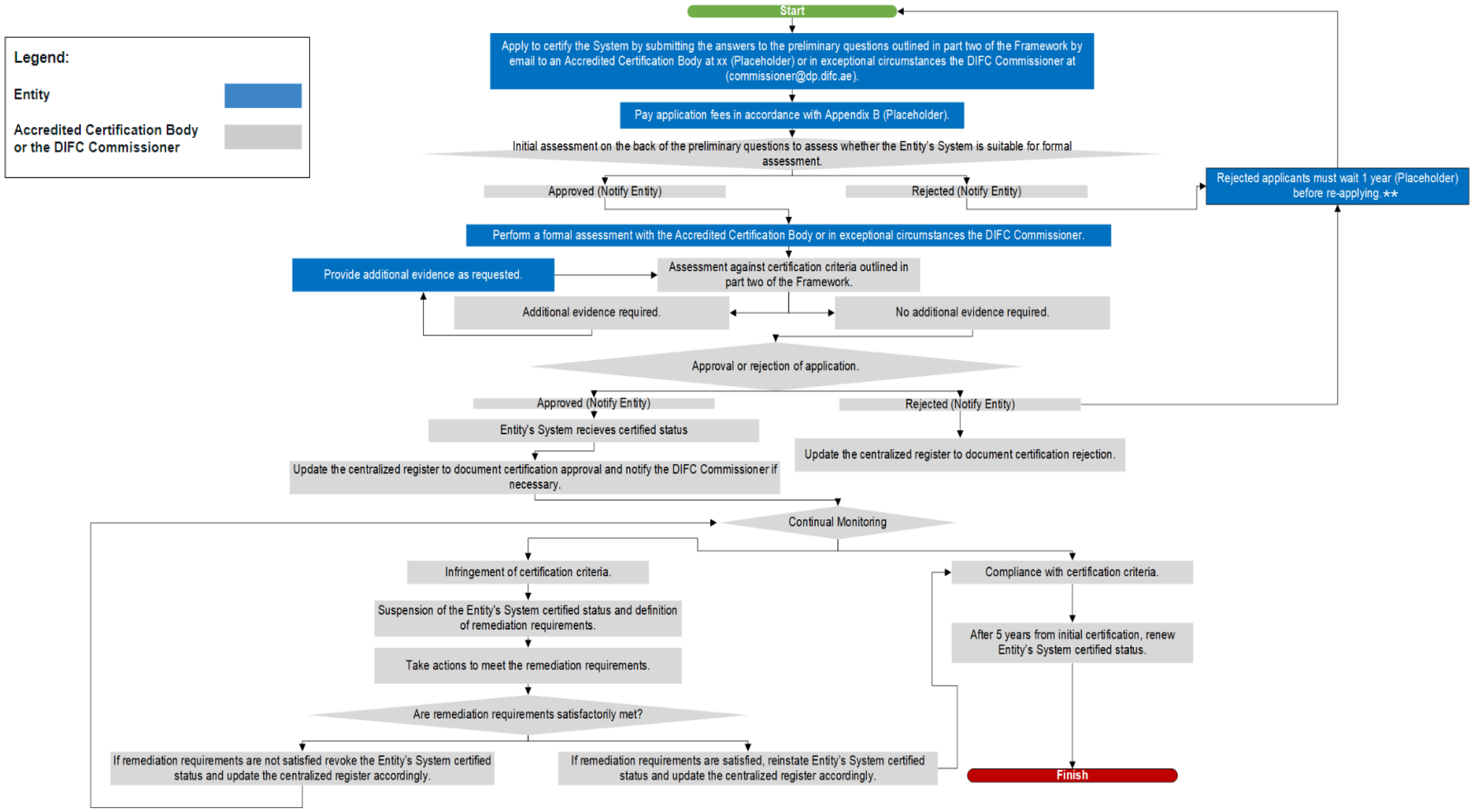
The Certification Applicant may wish to undergo an Article 20 Prior Consultation discussion regarding the System in order to secure an assessment by the Commissioner or his delegate(s) before going forward with deploying, operating or providing such System. For further information, please review the guidance and FAQs that accompany this Framework.

Preliminary Questions

- *Where is the Certification Applicant that is seeking certification of its System registered? (choices: within DIFC or Not registered in DIFC (provide location))*
- *In which industry does the Certification Applicant operate? (e.g., fintech and innovation, retail and leisure, non-financial services, etc)*
- *What System is the Certification Applicant deploying, providing or operating?*
- *Does the Certification Applicant's System process Personal Data?*
- *What type of Personal Data is the Certification Applicant's System Processing?*
- *Is the System used for High Risk Processing Activities?*
- *Will the System once developed or deployed be used or intended to be used by an Accredited Certification Body (its own organisation) or within the same group of companies as an Accredited Certification Body?*

Figure 2 – Systems Certification Process

*** Please note that exceptions may be granted by the Commissioner or responsible ACB. Where an exception is granted, it must be documented in accordance with the acceptance criteria set out in Appendix C.*



Systems Certification Program Requirements

The certification scheme criteria shall be met in full before an Accredited Certification Body can issue a certification for a Certification Applicant's System used for High Risk Processing Activities. As part of this Framework, relevant persons or Accredited Certification Bodies must be able to audit the certification of the relevant System or the System itself. In accordance with Regulation 10.3.3, compliance with each requirement shall be assessed in light of the chosen Certification Program Requirements agreed or selected by either the ACB, the CA or both, as well as the supporting documents provided.

As a reminder, the definitions of Deployers, Operators and Providers are found in Regulation 10.1.1:

> "Deployer" means, with respect to a System, the natural or legal person (i) under whose authority or on whose direction or for whose benefit the System is operated, or (ii) who receives the benefit of the operation of the System or any output generated by the System in each case without regard to whether or not the System is operated, supervised or hosted by such person, or such person defines or determines any of the purposes of which Personal Data is Processed by such System.
>
> "Operator" means a Provider that operates or supervises a System on behalf or otherwise for the benefit, and on the direction of a Deployer, in each case without regard to whether or not that Provider exercises any control over the Processing of Personal Data by the System.
>
> "Provider" means 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.

The Systems Certification Program Requirements below map to the Sample Detailed Certification Program Requirements found in Appendix C (the "Sample CPRs" or "Sample Certification Program Requirements"). If the Sample Requirements are not the basis of methodology or criteria agreed between the ACB and the CA, it is strongly encouraged that a mapping of the chosen CPR to the following Systems Certification Program Requirements is completed.

1 Principles Applicable to Deployers, Operators and Providers of Systems

Explanatory Note:

An Accredited Certification Body shall assess that the System used for High Risk Processing for commercial or other purposes meets specific evidentiary requirements and adheres, throughout the lifecycle of the System, to the fundamental principles of fairness, transparency, ethics, security, data quality, necessity and proportionality, risk-assessment and accountability.

Requirements:

1.1 An Accredited Certification Body shall assess that the System used to carry out High Risk Processing is deployed in accordance with an overarching governance document that details requirements for adherence to the principles of fairness, transparency, accountability, security, and ethics, or sufficiently similar concepts outlined in Regulation 10.3.1.

Examples of Acceptable Evidence

- *Framework or Policy documentation evidencing these fundamental principles.*

1.2 An Accredited Certification Body shall assess that a Certification Applicant seeking to certify its system has used a risk-based approach to determine the necessity of High Risk Processing of Personal Data through the System to be certified rather than through a different, lower risk System. If High Risk Processing through the System is deemed necessary, an Accredited Certification Body shall then assess:

1.2.1 whether identified risks of the System have been catalogued by the applicant, and where relevant, by the Accredited Certification Body;
1.2.2 whether collection and processing of Personal Data is necessary and proportionate for the purpose of the System use case; and
1.2.3 whether appropriate measures to effectively mitigate the impact of these elements are in place.

Examples of Acceptable Evidence

- *A Risk Management Framework evidencing commitment to identifying, assessing, categorising and mitigating risks.*

- *An AI Data Protection Impact Assessment that assesses the necessity of the Systems or at a minimum, of processing Personal Data in such Systems; identifies associated risks; includes management actions plans to address how controls have been integrated into*

development process (and evidence that controls have been integrated); and ensures compliance with the Law.

- *An AI Policy containing the necessary technical and organisational controls for the Systems, for example policies, procedures, and technical/organisational measures that demonstrate the requisite technical and organisational controls are in place for the Systems to sufficiently identify and mitigate high risks.*

- *A Risk Register containing all the associated risks of the Systems and supporting documentation showing associated high risks of the Systems have been identified and mitigated (in addition to or supporting AI DPIA set out above).*

1.3 An Accredited Certification Body shall assess that the System used for High Risk Processing is designed and will be implemented to be transparent and fair to data subjects about why their personal data is being collected, for what purpose(s), where it will be stored, whether it will be shared with third parties and any other information necessary to assist their ability to understand and choose whether to share such information. . Each Certification Applicant whose System is certified shall be able to provide evidence of meaningful notice and evidentiary explanations for its decisions around providing such information, incorporating the requirements set out in Article 29 and Regulation 10.2.2.

Examples of Acceptable Evidence

- *Privacy notice detailing the particulars of Personal Data Processing by the System in a clear and easily understandable manner, incorporating the elements of Regulation 10.2.2(a), particularly regarding the impact of the use of the System on the exercise of individual rights as provided under the Law in Article 29(1)(h)(ix).*

- *Privacy notice detailing the particulars of Personal Data Processing by the System in a clear and easily understandable manner, incorporating the elements of Regulation 10.2.2(b), particularly regarding the human-defined purposes for Processing, the human defined principles on the basis of which, and all human-defined limits within which, the System is capable of itself defining further purposes for Processing of Personal Data, and the codes, certifications or principles on which the Systems is designed or developed*

- *Consent mechanism of the System (where consent is relied upon as the lawful basis of Processing).*

- *Mechanism in place to update the System in response to user feedback.*

1.4 An Accredited Certification Body shall assess that accountability mechanisms are in place subject to an appropriate testing framework with supporting documentation that clearly delineates roles, responsibilities and System design regarding System data collection (fair and lawful process, purpose specification and compatibility, data minimisation and accuracy and security measures), as well as for monitoring the System and its outcomes. Any evidence of effective measures must demonstrate compliance with applicable regulations

and governance principles. Roles and responsibilities regarding transparency and other compliance obligations in the supply chain must be clear.

Examples of Acceptable Evidence

- *Policies and framework documentation outlining roles and responsibilities.*
- *Operating models that detail how monitoring activities are conducted.*
- *Employee training records related to monitoring Systems.*
- *Job descriptions of relevant personnel evidencing who is responsible for what in the monitoring process.*

- *Documentation containing the evidentiary requirements set out in Regulations 10.2.2(c) through Regulation 10.2.2(g), regarding System design materials demonstrating that it will seek human intervention and that the Certification Applicant certifying the System maintains or will maintain a register accounting for information including but not limited to information about Data Subjects' rights of access, lawful bases for Processing, automated decision making or contractual obligations of Joint Controllers, Processors or Sub-processors.*

1.5 An Accredited Certification Body shall assess that the System used for High Risk Processing is deployed with the appropriate measures in place to identify and mitigate risks of bias and discrimination.

Examples of Acceptable Evidence

- *A job description outlining education, training, or experience on ensuring fairness.*
- *Training programs related to reducing bias.*
- *Review and evaluation processes to identify and correct potential bias issues.*
- *Model modifications to address biases.*
- *Data quality assessments.*

1.6 An Accredited Certification Body shall assess that the System used for High Risk Processing is designed to ensure that to the extent possible, the data it processes and data sets are accurate, quality-assessed, reliable, relevant and limited to its specific purpose, and where required, human intervention to provide review and assurance is designed into the System.

Examples of Acceptable Evidence

- *Documentation of a data inventory evidencing that datasets used for training or operating the Systems are adequately sized and relevant, to be evaluated on a case-by-case basis where necessary.*
- *Documentation of the availability of metadata describing data sets used*
- *Documentation showing the use or implementation of privacy preserving methodologies that reduce the amount of personal data that needs to be collected, stored, or processed.*

- *Implemented measures in place to periodically review and update datasets to ensure its accuracy, quality, currency, relevance and reliability.*
- *Data/Statistical assessments verifying the currency and validity of data processed through Systems.*

1.7 An Accredited Certification Body shall assess that the System used for High Risk Processing is deployed with the appropriate level of security in place to protect personal data, maintaining confidentiality, and preventing data breaches that could cause reputational, psychological, financial, professional, or other types of harm.

Examples of Acceptable Evidence

- *Security risk assessments to identify potential vulnerabilities in the System.*
- *Model debugging processes rectifying any flaws or vulnerabilities in the System.*
- *Data breach policies and procedures evidencing the ability to respond effectively in the event of a security incident.*
- *Data encryption and access controls safeguarding personal data processed through Systems.*
- *Deployment of privacy-enhancing technologies (PETs) where appropriate.*
- *Certification or compliance documentation demonstrating adherence to internationally recognised standards or best practices pertaining to security measures e.g. applicable ISO standards.*

1.8 An Accredited Certification Body shall assess that the Certification Applicant seeking certification of a System has measures in place for active monitoring of the use and quality of the collected personal data, as well as for review or regular model tuning when appropriate (e.g., changes to customer behaviour, commercial objectives, risks, and corporate values), as well as a mechanism for providing or receiving updates to or from third parties (processors, users, etc) about the quality and use of personal data that is collected via the System or by other relevant, lawful methods.

Examples of Acceptable Evidence

- *Documentation of procedures to ensure that the System is updated with new data points, for example via an automated pipeline designed to update the system with newer data points via the extraction, transformation, and loading (ETL) process, and to retrain the model(s) periodically when new data points are added.*

- *Procedures for gathering feedback from AI system users via multiple channels (i.e., where appropriate and permissible by law or via end user opt-in, through the use of mail distribution lists, in-app feedback, and periodic user discussion forums)*

- *Procedures for updating the database as well as any providing or receiving updates to / from processors or other third parties in receipt of the personal data*

2 Third Parties and Compliance

Explanatory Note:

An Accredited Certification Body shall assess the System used for High Risk Processing on its procurement, compliance and resilience practices, particularly when third parties such as Sub-processors are appointed.

2.1 An Accredited Certification Body shall assess that the System used for High Risk Processing has, where applicable, been promulgated, developed, designed or otherwise procured subject to enhanced due diligence, ensuring that appropriate technical, organisational or relevant contractual arrangements are in place to safeguard Personal Data, and that processors or other third parties related to the function of the System will implement substantially similar measures.[4]

Examples of Acceptable Evidence

- *Due diligence documentation, recording the process for assessing Provider's Systems and their compliance with the Law.*
- *Contracts or agreements with Providers, clearly delineating data protection roles and responsibilities.*
- *Contracts or agreements for international data transfers for Systems, including safeguards for cross-border data flows and compliance with the Law.*
- *Review of the System Provider's, Data Protection by Design Documentation, evidencing the Provider's adherence to data protection principles.*

2.2 An Accredited Certification Body shall assess that the Systems used for High Risk Processing are robust and resilient, guarding against unauthorised access that may exploit vulnerabilities and against faults or errors arising from changes in the System's environment.

Examples of Acceptable Evidence

- *Policies and procedures to prevent cyber-attacks such as data poisoning.*
- *Security architecture documentation outlining controls to safeguard against various types of attacks.*
- *Training materials or programs educating personnel on recognising and mitigating potential attacks.*
- *Documentation of error handling mechanisms and contingency plans.*
- *Incident reports.*

[4] Please see Guidance on Article 24 Contract Clauses

- *Certification or compliance documentation demonstrating adherence to internationally recognised standards or best practices pertaining to security measures e.g. applicable ISO standards.*

2.3 An Accredited Certification Body shall assess that the System used for High Risk Processing acts in accordance with technical and organisational measures as well as appropriate safeguards and controls, including but not limited to disposal, vulnerability / attack detection, resilience or failure of Human-defined processing purposes. Any Self-defined purposes generated by the System, i.e. automated decision-making, shall conform to a predefined set of human approved principles.

Examples of Acceptable Evidence

- *System architecture documentation.*
- *Code review records showing assessments of how the code implements human-defined processing purposes and the absence of self-defined purposes.*
- *Processing purpose logs tracking the processing purposes of the system, documenting how data is being processed and ensuring that it's in line with human-defined purposes.*
- *Documentation of externally predefined principles and how the System conforms to them.*
- *Internal policies and procedures outlining how the system should operate and the principles it should follow, ensuring that it aligns with human-defined processing purposes.*
- *Algorithmic audits showing the assessment of the algorithms against human-defined processing purposes and any corrective actions taken.*

2.4 An Accredited Certification Body shall assess that the System used for High Risk Processing complies by design or by default with the Law and Regulations, observing that the Certification Applicant using the System demonstrates legitimate and lawful processing of Personal Data.

Examples of Acceptable Evidence:

- *Any documents evidencing compliance with the Law and Regulations.*
- *Policies or procedures for responding to government authority requests in accordance with Article 28 or similar due diligence obligations.*
- *Compliance audits, risk register, gap assessments mitigation measures to demonstrate compliance with the Law and Regulations.*

3 Governance and Oversight

Explanatory Note:

An Accredited Certification Body shall assess that the System adheres to specific governance and oversight requirements.

3.1 An Accredited Certification Body shall assess that the System used for High Risk Processing is or will be monitored by an Automated Systems Officer (ASO), who will have at a minimum the same or similar competencies, status, role and tasks of a Data Protection Officer (DPO) as set out in Articles 16, 17 and 18 of the Law and in relevant guidance. To distinguish the roles of DPO or similar, the ASO shall have the technical and organisational expertise to ensure effective governance and oversight of the System and ongoing validity of the certification of the System.[5]

Examples of Acceptable Evidence

- *Job Profile/Description of the ASO which specifies technical knowledge of Systems, ethics, data protection, risk management, complaints handling and remediation, regulatory requirements and legal requirements.*

- *Specific requirements of ASO or similar position from documented international best practice guidance or frameworks*

3.2 An Accredited Certification Body shall assess that the System is subject to mechanisms administered by the Certification Applicant seeking certification of the System that assure routine review of its processing purposes, including the output which the System produces on the basis of such Processing and the manner in which such output is used, ensuring human oversight throughout.

Examples of Acceptable Evidence

- *Documentation of oversight processes, including measures for receiving, investigating and responding to complaints about the System's function and outputs.*
- *Audits and review reports detailing the processing purposes and human oversight.*
- *Training records ensuring the personnel are adequately trained to provide oversight.*
- *Feedback logs to capture feedback on the processing purposes of the system.*
- *System adaptations to maintain alignment with intended processing purposes.*
- *Ethics committee.*

[5] Please see Guidance and FAQs for Regulation 10

3.3 An Accredited Certification Body shall ensure that the Certification Applicant seeking certification of its System will only indicate that it is duly and validly certified as long as the certification is valid and has not expired, been revoked, modified such that certification is no longer valid or otherwise no longer exists regarding the System. Additional oversight and review are required where the certified System is developed or deployed by a Certification Applicant in its own organisation or within the same group of companies as an Accredited Certification Body, such that it monitors and documents any conflicts of interests regarding the certification and takes appropriate recourse to seek independent confirmation that the certification is valid in any case.

Examples of Acceptable Evidence

- *Code of Conduct of Accredited Certification Body and Certification Applicant seeking certification of the System*
- *Conflicts of Interest Complaints Handling and reporting procedures and policies of Accredited Certification Body and Certification Applicant seeking certification of the System*
- *Confirmation by Accredited Certification Body and Certification Applicant seeking certification of the System of compliance with Regulation 6.2 regarding Unfair or Deceptive Practices*

4 Audit Criteria

4.1 Audit criteria shall be met in full for an Accredited Certification Body or in exceptional cases for the Commissioner to confirm ongoing compliance with Regulation 10.3.3 of a Certification Applicant's System for High Risk Processing Activities, i.e., compliance with the above certification requirements.

4.2 Confirmation through audit of the effectiveness of the certification shall be assessed periodically, at least once in during the three (3) year validity of the Certification.

4.3 The audit criteria will ensure that the Certification Applicant seeking certification of the System:

4.3.1 Maintains consistent and up-to-date documentation showing that the System is tested regularly against the certification requirements;

4.3.2 Can show any indicators, marks or symbols regarding certification are displayed in accordance with applicable laws and regulations, including but not limited to Regulation 6.2 regarding Unfair or Deceptive Practices or application Intellectual Property laws and regulations;

4.3.3 Regularly review of the necessity and proportionality of requirements for use of a System that is used for High Risk Processing; and

4.3.4 Documents upgrades or changes in System architecture that maintain or improve the safeguards in place to ensure protection and transparency of System functionality;

4.3.5 Has Appointed an Autonomous Systems Officer (ASO) and it can be proven that there was no more than a gap of one month before the operation of a System for High Risk Processing or between a replacement ASO appointment, unless an exception to this rule for extenuating circumstances is approved by the Commissioner, unless an exception to this rule for extenuating circumstances is approved by the Commissioner;

4.3.6 Provides appropriate support to assure that the ASO may independently review and assess the audit documentation against the certification requirements, and a gap analysis, risk register, and management action plan are provided where required in order to remedy such risks; and

4.3.7 Anything else the Accredited Certification Body or on a case-by-case basis, the Commissioner, deems appropriate to inspect.

4.4 If during the course of the Certification assessment, the Accredited Certification Body deems through its own risk assessment methodology that the compliance audit should be conducting more frequently, it must notify the Certification Applicant seeking Certification of its System(s) no less than thirty (30) days prior to the compliance audit.

4.5 The above actions do not preclude the DIFC Data Protection Commissioner's Office from inspecting the Certification Applicant for general compliance with the Law and Regulations in accordance with its own inspection form and methodology.

Appendix A – Templates

All templates are available upon request from the Commissioner or relevant delegate.

Application for Accredited Certification Body – to be completed by Certification Applicant seeking to become an Accredited Certification Body in accordance with Article 51 of the Law.

Application for Certification – to be completed by Certification Applicant whose System(s) will be certified by an Accredited Certification Body.

Confirmations -

- Authorised Signatory
- Compliance with applicable laws and regulations (including Reg 6.2)
- Conflict / No conflict of interests
- Validity of certification awarded

Accreditation Application Acceptance / Cancellation / Renewal / Revocation Report - to be completed by the Commissioner or his delegate(s) in order to provide reasons and any conditions for awarding or not awarding accreditation in accordance with Article 51 of the Law. This report must be completed within 3 months of the accreditation criteria review and assessment for the particular circumstance.

Certification Application Acceptance Report – to be completed by an Accredited Certification Body upon completing the review of an application for certification. This report must be completed within 3 months of the certification criteria review and assessment.

Certification Program Requirements / Program Requirements – to be completed by a Certification Applicant seeking to certify its System in accordance with Regulation 10.3.3, either in the form prescribed by the Commissioner, as per the tables in Appendix C or as per Certification Program Requirements that align with either form.

Process for providing statistics on the types of complaints – to be provided by ACB

Process for releasing anonymous case notes on a selection of resolved complaints – to be provided by ACB

Appendix B – Accredited Certification Body Application Acceptance Report

This Accreditation Application Acceptance Report (the "AAA Report") reflects the full and final decision of the Commissioner regarding the award of accreditation to [_____], an Accredited Certification Body. Based on the findings in this AAA Report, an Accredited Certification Body may, for a period of five (5) years, hold itself out as an Accredited Certification Body in accordance with Article 51 and Article 51 of the Law and accompanying Regulations, for the purposes of certifying Systems in accordance with Regulation 10 therein.

ACCREDITED CERTIFICATION BODY RECOGNITION CRITERIA CHECKLIST

The following checklist corresponds with the nine (9) areas of accreditation recognition criteria for Applicant Accredited Certification Bodies:

1 *Independence*
2 *Expertise in relation to the subject-matter of the certification*
3 *Written Undertakings*
4 *Established procedures*
5 *Transparency, complaints handling and dispute resolution*
6 *Absence of conflict of interest*
7 *Communicating with the Commissioner*
8 *Certification Application Review process*
9 *Criteria Review Mechanisms*

Independence / Conflicts of Interest

☐ Applicant Accredited Certification Body should describe how requirements Part 1, Section 6 have been met and submit all applicable written policies and documentation.

☐ Applicant Accredited Certification Body should submit an overview of the internal structural and procedural safeguards to address any of the potential or actual conflicts of interest identified in Part 1, Section 6.

☐ Applicant Accredited Certification Body should describe the disclosure/withdrawal mechanisms to be used in the event of any actual conflict of interest identified.

Expertise / Model Program Requirements

☐ Applicant Accredited Certification Body should indicate whether the program requirements against which it intends to assess the System, as well as its expertise in conducting such assessment.

Certification Review Process / Mechanisms

☐ Applicant Accredited Certification Body should submit a description of how the requirements as identified in Part 1, Section 8 have been met.

Established Procedures for On-going Monitoring and Compliance Review Processes

☐ Applicant Accredited Certification Body should submit a description of written procedures to ensure the integrity of the certification process and to monitor the participant's compliance with the requirements described in Part 1, Sections 3 to 5 and Section 8.

☐ Applicant Accredited Certification Body should describe the review process to be used in the event of a suspected breach of the Certification Program Requirements described in Part 1, Sections 3 to 5 and Section 8

Established Procedures for Re-Certification and Annual Attestation

☐ Applicant Accredited Certification Body should describe their re-certification and review process as identified in Part 1, Section 4.

Dispute Resolution Process

☐ Applicant Accredited Certification Body should describe the mechanism to receive and investigate complaints and describe the mechanism for cooperation with other DIFC recognised Accredited Certification Bodies that may be used when appropriate.

☐ Applicant Accredited Certification Body should describe how the dispute resolution process meets the requirements identified in Part 1, Section 5, whether supplied directly by itself or by a third party under contract (and identify the third-party supplier of such services if applicable and how it meets the conflict of interest requirements identified in Part 1, Section 6) as well as its process to submit the required information.

Mechanism Established Procedures for Enforcing Program Requirements

☐ Applicant Accredited Certification Body should provide an explanation of its authority to enforce its program requirements.

☐ Applicant Accredited Certification Body should describe the policies and procedures for notifying a participant of non-compliance with Certification Applicant's program requirements and provide a description of the processes in place to ensure the participant remedy the non-compliance.

☐ Applicant Accredited Certification Body should describe the policies and procedures regarding penalties identified in Part 1, Section 4.

☐ Applicant Accredited Certification Body should describe its policies and procedures for referring matters to the appropriate public authority or enforcement agency for review and possible law enforcement action. [NOTE: immediate notification of violations may be appropriate in some instances].

☐ Applicant Accredited Certification Body should describe its policies and procedures to respond to requests from enforcement entities in other jurisdictions where possible.

Table 1: Criteria for acceptance of Independence evidence:

Accreditation Requirement	**Evidence**	**Acceptance Methodology**	**Assessment**
Explanatory Note: An Accredited Certification Body shall be assessed on its ability to demonstrate its functional, material / financial and organisational and accountability-based decision-making independence. *Requirements: An Accredited Certification Body shall demonstrate to the satisfaction of the Commissioner its independence in general regarding the subject matter of the certification proposed and from the Commissioner or his delegates.*	[List Evidence Provided]	Basic: Current, valid evidence has been provided and is sufficient to meet this requirement. Weighted / Rated: In considering the evidence, the Commissioner will base his decision on the weight and frequency of factors that create or negate undue pressure or influence on personnel. Such factors may include the stability of governance processes within the applicant organisation regarding changes or shifts in resources requirements, KPIs or third-party engagement	The evidence provided is: - Accepted - Accepted with conditions - Rejected - Rejected but may re-apply within three (3) months to one (1) year.

Conditions of acceptance:

[Outline here, at Commissioner's discretion]

Reasons for Rejection:

[Outline here, at Commissioner's discretion]

Table 2: Criteria for acceptance of Expertise evidence:

Accreditation Requirement	Evidence	Acceptance Methodology	Assessment
Explanatory Note: An Accredited Certification Body shall be assessed on its ability to demonstrate its expertise in accordance with this section of the criteria. Expertise requirements take into account various factors such as the specific sector of the criteria, the size of the sector, the number of committees within the sector, the risks tied to the Processing activities and the different interests at stake. *Requirements:* An Accredited Certification Body shall demonstrate to the satisfaction of the Commissioner its expertise in relation to the subject matter of the certification, in this case, the safe and ethical use of autonomous or semi-autonomous systems for use in High Risk Processing Activities itself.	[List Evidence Provided]	In considering the evidence for understanding and experience, the Commissioner will base his decision on the authority of the resources provided to substantiate the quality of knowledge and understanding as well as the extent of experience regarding assessing risks and impact of HRP. Such factors may include the type of professional standards / professional standards body upon which the evidence is based; the source and reputation of entities providing any testimonials, or other relevant, globally recognised accreditations. In considering the evidence for governance and controls, the Commissioner will base his decision on the authority substantiating industry best practices.	The evidence provided is: - Accepted - Accepted with conditions - Rejected - Rejected but may re-apply within three (3) months to one (1) year.

Conditions of acceptance:

[Outline here, at Commissioner's discretion]

Reasons for Rejection:

[Outline here, at Commissioner's discretion]

Table 3: Criteria for acceptance of Written Undertakings evidence:

Accreditation Requirement	**Evidence**	**Acceptance Methodology**	**Assessment**
Explanatory Note: An Applicant Accredited Certification Body shall be assessed on its commitment to adhere to the relevant Certification Program Requirements and to applicable laws. *Requirements:* An Applicant Accredited Certification Body shall formally commit in writing to adhere to the program requirements of the relevant certification scheme it applies to a System assessment, on a case-by-case basis, and to respect the criteria of the proposed scheme. It must also confirm that it in completing the assessment as well as in applying the assessment criteria, it will comply with applicable laws, including intellectual property laws governing the use of relevant marks regarding certification, if any.	[List Evidence Provided]	Basic: Current, valid evidence has been provided and is sufficient to meet this requirement. Weighted / Rated: In considering the evidence, the Commissioner will base his decision on the clarity and conformity of the written undertakings provided.	The evidence provided is: - Accepted - Accepted with conditions - Rejected - Rejected but may re-apply within three (3) months to one (1) year.

Conditions of acceptance:

[Outline here, at Commissioner's discretion]

Reasons for Rejection:

[Outline here, at Commissioner's discretion]

Table 4: Criteria for acceptance of Established Procedures evidence:

Accreditation Requirement	**Evidence**	**Acceptance Methodology**	**Assessment**
Explanatory Note: An Applicant Accredited Certification Body shall be assessed on established procedures for the issuing, periodic review / re-certification, and withdrawal of certification, enforcement of certification requirements, and use of seals, and marks in connection with the proposed certification scheme. It must demonstrate whether the monitoring tasks and duties it carries out are regular, timely and complete. The monitoring procedures implemented by an Applicant Accredited Certification Body shall be in accordance with this framework. *Requirements:* An Applicant Accredited Certification Body shall demonstrate that it has a relevant procedure to check the eligibility of Certification Applicants to apply for certification of its System and their staff, its ability to comply with criteria and subsequently the issuance or withdrawal of the certification awarded.	[List Evidence Provided]	Basic: Current, valid evidence has been provided and is sufficient to meet this requirement. Weighted / Rated: In considering the evidence, the Commissioner will base his decision on the clarity and conformity of the Applicant ACBs internal procedures, examples of internal supervision and enforcement mechanisms (if any) and overall technical and organisational compliance framework.	The evidence provided is: - Accepted - Accepted with conditions - Rejected - Rejected but may re-apply within three (3) months to one (1) year.

Conditions of acceptance:

[Outline here, at Commissioner's discretion]

Reasons for Rejection:

[Outline here, at Commissioner's discretion]

Table 5: Criteria for acceptance of Transparency, complaints handling and dispute resolution evidence:

Accreditation Requirement	Evidence	Acceptance Methodology	Assessment
Explanatory Note: An Applicant Accredited Certification Body shall be assessed on the procedures implemented to process complaints and appeals regarding infringements of the certification of a Certification Applicant's certified System or the manner in which the certification has been or is being implemented. The Certification Body Application must demonstrate that it will make those procedures and structures transparent to Data Subjects and the public. *Requirements:* An Applicant Accredited Certification Body must demonstrate that it shall provide evidence of a procedure to handle complaints about a Certification Applicant's certified System or from any Data Subject whose Personal Data is processed by a System. This process for complaints handling and decision-making shall be publicly available, accessible and easily understood.	[List Evidence Provided]	Basic: Current, valid evidence has been provided and is sufficient to meet this requirement. Weighted / Rated: In considering the evidence, the Commissioner will base his decision on the objectivity, clarity and conformity of the Applicant ACBs transparency, complaints and dispute resolution procedures.	The evidence provided is: - Accepted - Accepted with conditions - Rejected - Rejected but may re-apply within three (3) months to one (1) year.

Conditions of acceptance:

[Outline here, at Commissioner's discretion]

Reasons for Rejection:

[Outline here, at Commissioner's discretion]

Table 6: Criteria for acceptance of evidence regarding ACB's Absence of Conflicts of Interests processes:

Accreditation Requirement	**Evidence**	**Acceptance Methodology**	**Assessment**
Explanatory Note: An Applicant Accredited Certification Body must be free of actual or potential conflicts of interest in order to participate in the Regulation 10 Accreditation and Certification Framework. For the purposes of participation as an Accredited Certification Body, this means the ability of an Accredited Certification Body to perform all tasks related to a Certification Applicant's certification free from influences that would compromise an Accredited Certification Body's professional judgment, objectivity and integrity. *Requirements:* An Applicant Accredited Certification Body's personnel shall comply with all requirements set out in herein and shall report to the relevant, authorised person or persons, including but not limited to the Commissioner or other designated application reviewer, where required, any situation likely to create a conflict of interest.	[List Evidence Provided]	Basic: Current, valid evidence has been provided and is sufficient to meet this requirement. Weighted / Rated: In considering the evidence, the Commissioner will base his decision on the clarity and thoroughness of the Applicant ACBs conflicts of interests handling procedures.	The evidence provided is: - Accepted - Accepted with conditions - Rejected - Rejected but may re-apply within three (3) months to one (1) year.

Conditions of acceptance:

[Outline here, at Commissioner's discretion]

Reasons for Rejection:

[Outline here, at Commissioner's discretion]

Table 7: Criteria for acceptance of evidence regarding ACB's Communications with the Commissioner:

Accreditation Requirement	Evidence	Acceptance Methodology	Assessment
Explanatory Note: An Applicant Accredited Certification Body shall be assessed on whether it can provide information outlined in this section of the criteria regarding communications and reporting to the DIFC Commissioner on a regular basis about status of certified bodies and acceptable certification program requirements for updates to the register required by Article 50(5). *Requirements:* An Applicant Accredited Certification Body shall provide evidence of a clear mechanism that governs reporting any suspensions or revocations of a Certification Applicant's certified System to the Commissioner. Please see Part 1, Section 7 for further information.	[List Evidence Provided]	Basic: Current, valid evidence has been provided and is sufficient to meet this requirement. Weighted / Rated: In considering the evidence, the Commissioner will base his decision on the clarity and thoroughness of the Applicant ACBs communications plans and procedures.	The evidence provided is: - Accepted - Accepted with conditions - Rejected - Rejected but may re-apply within three (3) months to one (1) year.

Conditions of acceptance:

[Outline here, at Commissioner's discretion]

Reasons for Rejection:

[Outline here, at Commissioner's discretion]

Table 8: Criteria for acceptance of evidence regarding ACB's Certification Application Review processes:

Accreditation Requirement	**Evidence**	**Acceptance Methodology**	**Assessment**
Explanatory Note: An Applicant Accredited Certification Body shall be assessed on its certification application acceptance process to ensure consistency with relevant program requirements during the application process, as well as its ongoing monitoring and compliance review processes once certification has been awarded to a Certification Applicant. *Requirements:* An Applicant Accredited Certification Body must have a comprehensive process to review a Certification Applicant's policies and practices with respect to its compliance with Regulation 10 and the Law, and to verify its compliance with the Accredited Certification Body's Certification Program Requirements (the "Certification Review Process").	[List Evidence Provided]	Basic: Current, valid evidence has been provided and is sufficient to meet this requirement. Weighted / Rated: In considering the evidence, the Commissioner will base his decision on the clarity and thoroughness of the Applicant ACBs certification application update and review procedures.	The evidence provided is: - Accepted - Accepted with conditions - Rejected - Rejected but may re-apply within three (3) months to one (1) year.

Conditions of acceptance:

[Outline here, at Commissioner's discretion]

Reasons for Rejection:

[Outline here, at Commissioner's discretion]

Table 9: Criteria for acceptance of evidence regarding ACB's Certification Program Requirements Review Mechanisms:

Accreditation Requirement	**Evidence**	**Acceptance Methodology**	**Assessment**
Explanatory Note: An Applicant Accredited Certification Body, once it is awarded accreditation and becomes and Accredited Certification Body shall be periodically assessed by the Commissioner or his delegate on whether it actively participates in any further development or extension of the Certification Program Requirements' scope and/or its content, i.e., for the purposes of continuous improvement based on current technology developments, regulation or best practices. *Requirements:* An Accredited Certification Body, once accredited, shall contribute to reviews of the overall Framework, or of the Certification Program Requirements, as needed or upon request of the Commissioner. It shall therefore ensure that upon application for accreditation, it can demonstrate that it has documented plans and procedures to conduct regular reviews to ensure that both Certification Program Requirements and this Framework (where feedback is requested) remain relevant to certifying Systems and that Certification Applicants with a certified System continue to meet requirements of DIFC Regulation 10 as updated from time to time.	[List Evidence Provided]	Basic: Current, valid evidence has been provided and is sufficient to meet this requirement. Weighted / Rated: In considering the evidence, the Commissioner will base his decision on the clarity and thoroughness of the ACBs Certification Program Requirements review process.	The evidence provided is: - Accepted - Accepted with conditions - Rejected - Rejected but may re-apply within three (3) months to one (1) year.

Conditions of acceptance:

[Outline here, at Commissioner's discretion]

Reasons for Rejection:

[Outline here, at Commissioner's discretion]

Appendix C – Certification Application Acceptance Report

This Certification Application Acceptance Report ("CAA Report") reflects the full and final decision of an Accredited Certification Body regarding certification of [SYSTEM], applied for by [CERTIFICATION APPLICANT]. Based on the findings in this CAA Report, [CERTIFICATION APPLICANT] may, for a period of three (3) years, hold [SYSTEM] out as Certified in accordance with Article 50 of the Law, and accompanying Regulations, for the purposes of certifying Systems in accordance with Regulation 6.2 and Regulation 10 therein.

Sample Detailed Certification Program Requirements

A Certification Applicant seeking to certify its System, i.e., the Certification Applicant, may present to the Accredited Certification Body its request to be assessed against a certification scheme that meets or exceeds the following detailed Certified Program Requirements, which corresponds with the broad objectives set out in Part 2 of this Framework.

1 *Obligations of Deployers, Operators and Providers of Systems Regarding Purposes and Principles*
2 *Third Parties and Compliance*
3 *Governance and Oversight*
4 *Audit Criteria*

If the Certification Applicant does not request any Certification Program Requirements, then the Accredited Certification Body may recommend or agree with the Certification Applicant the appropriate Certification Program Requirements for assessment that align with the Certification Program Requirements below. In limited cases, the Commissioner may recommend Certification Program Requirements under consultation, in accordance with Article 21 of the Law.

The following sample Certification Program Requirements form the basis of a robust, complete privacy by design program that would satisfy Part 2 of the Regulation 10 Audit and Certification Program Requirements. Where these criteria are utilised, an Accredited Certification Body must review and where necessary interrogate each criterion in order to appropriately certify the System. If a different audit and set of Certification Program Requirements are used, the Accredited Certification Body must interrogate it in accordance with the criteria below and may take reasonable action to align or map the proposed Certification Program Requirements accordingly, and reasonable costs for doing so may be allocated to the Certification Applicant.

SECTION 0: PREVENTING HARM

Assessment Purpose -. *Recognising the interests of the individual to legitimate expectations of data protection and privacy, Certification Applicant's personal information protection program should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.*[6]

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement (*evidence provided to meet assessment criteria)***
0. Are the Certification Applicant's (CA's) organisational controls designed to prevent harms resulting from the wrongful collection or misuse of personal information, as well as proportionate to the likelihood and severity of any harm threatened by the collection, use or transfer of personal information? ***MAP TO PART 2 CPRs:*** Section 1, CPR 1.1, 1.2	Data protection and privacy approaches, including self-regulatory efforts, education and awareness campaigns, laws, regulations, and enforcement mechanisms, should be designed to prevent harm to individuals from the wrongful collection and misuse of their personal information. Where there has been a significant security breach affecting personal information, it may help to reduce the risk of harmful consequences to the individuals concerned to give notice to Privacy Enforcement Authorities and/or the individuals concerned. If **YES,** an Accredited Certification Body must verify that the Certification Applicant's privacy practices and policy include the following characteristics: • Provisions for compliance with Regulation 6.2 • Is in accordance with the principles of the [LAW] ; • Is easy to find and accessible. • Applies to all personal information, whether collected online or offline. Where Certification Applicant answers **NO** to question 0, the Accredited Certification Body must inform the Certification Applicant that such policies as described herein are required for compliance with this principle.	

SECTION 1: NOTICE

Assessment Purpose – *To ensure that individuals understand the Certification Applicant's personal information policies (subject to any qualifications) and controls where the Certification Applicant wishes to use, operate, provide, offer or otherwise make available for commercial use a System to engage in High Risk Processing Activities, including to whom the personal information may be transferred in due course, or the purpose for which the personal information may be used. Refer to [Appendix C1][7] for a list of acceptable Qualifications to the provision of notice.*

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement (*evidence provided to meet assessment criteria)***
1. Does the CA provide clear and easily accessible statements about its practices and policies that govern the personal information described above (a "Privacy Statement")? Where YES, provide a copy of all applicable Privacy Statements and/or hyperlinks to the same. *MAP TO PART 2 CPRs:* Section 1, CPR 1.3 (for all sub-questions)	If **YES,** an Accredited Certification Body must verify that the Certification Applicant's privacy practices and policy (or other Privacy Statement) include the following characteristics: • Available on the Certification Applicant's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified). • Is in accordance with the principles of the [LAW] ; • Is easy to find and accessible. • Applies to all personal information, whether collected online or offline. • States an effective date of Privacy Statement publication. Where Certification Applicant answers **NO** to question 1 and does not identify an applicable qualification subject to the Qualifications to Notice set out below, an Accredited Certification Body must inform the Certification Applicant that Notice as described herein is required for compliance with this principle. Where the Certification Applicant identifies an applicable qualification, an Accredited Certification Body must verify whether the applicable qualification is justified.	

[7] Originally referred to this https://privacy.gov.ph/wp-content/uploads/2022/04/Cross-Border-Privacy-Rules-Intake-Questionnaire.pdf

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement (*evidence provided to meet assessment criteria)***
1.a) Does this Privacy Statement describe how personal information is collected?	If **YES**, an Accredited Certification Body must verify that: • The statement describes the collection practices and policies applied to all covered personal information collected by the Certification Applicant. • the Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and • The Privacy Statement reports the categories or specific sources of all categories of personal information collected. If **NO**, an Accredited Certification Body must inform the Certification Applicant that Notice as described herein is required for compliance with this principle.	
1.b) Does this Privacy Statement describe the purpose(s) for which personal information is collected?	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify that the Certification Applicant provides notice to individuals of the purpose for which personal information is being collected. Where the Certification Applicant answers **NO** and does not identify an applicable qualification set out below, an Accredited Certification Body must notify the Certification Applicant that notice of the purposes for which personal information is collected is required and must be included in their Privacy Statement. Where the Certification Applicant identifies an applicable qualification, an Accredited Certification Body must verify whether the applicable qualification is justified.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement (*evidence provided to meet assessment criteria)***
1.c) Does this Privacy Statement inform individuals whether their personal information is made available to third parties and for what purpose?	Where the Certification Applicant answers YES, an Accredited Certification Body must verify that the Certification Applicant notifies individuals that their personal information will or may be made available to third parties, identifies the categories or specific third parties, and the purpose for which the personal information will or may be made available. Where the Certification Applicant answers **NO** and does not identify an applicable qualification, an Accredited Certification Body must notify the Certification Applicant that notice that personal information will be available to third parties is required and must be included in their Privacy Statement. Where the Certification Applicant identifies an applicable qualification, an Accredited Certification Body must verify whether the applicable qualification is justified.	
1.d) Does this Privacy Statement disclose the name of the applicant's company and location, including contact information regarding practices and handling of personal information upon collection? Where YES please describe.	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify that the Certification Applicant provides name, address and a **functional** e-mail address. Where the Certification Applicant answers **NO** and does not identify an applicable qualification, an Accredited Certification Body must inform the Certification Applicant that such disclosure of information is required for compliance with this principle. Where the Certification Applicant identifies an applicable qualification, an Accredited Certification Body must verify whether the applicable qualification is justified.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement (*evidence provided to meet assessment criteria)***
1.e) Does this Privacy Statement provide information regarding the use and disclosure of an individual's personal information?	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify that the Certification Applicant's Privacy Statement includes, if applicable, information regarding the use and disclosure of all personal information collected. Refer to question 8 for guidance on permissible uses of personal information. Where the Certification Applicant answers **NO** and does not identify an applicable qualification, an Accredited Certification Body must inform the Certification Applicant, that such information is required for compliance with this principle. Where the Certification Applicant identifies an applicable qualification, an Accredited Certification Body must verify whether the applicable qualification is justified.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement (*evidence provided to meet assessment criteria)***
1.f) Does this Privacy Statement provide information regarding whether and how an individual can access and correct their personal information?	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify that the Privacy Statement includes: • The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means). • The process that an individual must follow in order to correct his or her personal information Where the Certification Applicant answers **NO** and does not identify an applicable qualification, an Accredited Certification Body must inform the Certification Applicant that providing information about access and correction, including the Certification Applicant's typical response times for access and correction requests, is required for compliance with this principle. Where the Certification Applicant identifies an applicable qualification, an Accredited Certification Body must verify whether the applicable qualification is justified.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement (*evidence provided to meet assessment criteria)***
1.g) In addition to any notices, where CA is providing or using an application or website service employing Systems to Process Personal Data, does it maintain a register that may be made available upon request by any relevant party, that lists information including but not limited to: (i) use cases, necessity and proportionality of Processing activities, or Processing activities or categories in which such Systems are used, (ii) how information in the System can be accessed by Data Subjects in accordance with Articles 32 to 40 of the Law; (iii) whether the System will be used solely to make automated decisions (iv) with which Third Parties or, to the extent permitted by applicable laws, which Requesting Authorities any Personal Data used in the Systems is Processed as part of stable arrangements, other than on an occasional basis; (v) with which Third Parties or, to the extent permitted by applicable laws, which Requesting Authorities, any Personal Data used in the Systems is Processed in accordance with one or more of the lawful bases set out in Article 10 or Article 11 of the Law; (vi) contractual obligations of Joint Controllers, Processors or Sub-processors; and (vii) where Third Parties or Regulatory Authorities engaged in Processing Personal Data used in the Systems are located and appropriate safeguards for exporting the Personal Data	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify that the Autonomous Systems Register includes the information required in Regulation 10.2.2(g) Where the Certification Applicant answers **NO** and does not identify an applicable qualification, an Accredited Certification Body must inform the Certification Applicant that providing information that is required for compliance with this principle. Where the Certification Applicant identifies an applicable qualification, an Accredited Certification Body must verify whether the applicable qualification is justified.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement (*evidence provided to meet assessment criteria)***
2. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting for the CA), does the CA provide notice that such information is being collected? *MAP TO PART 2 CPRs:* Section 1, CPR 1.1, 1.2	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify that the Certification Applicant provides notice to individuals that their personal information is being (or, if not practicable, has been) collected and that the notice is reasonably available to individuals. Where the Certification Applicant answers **NO** and does not identify an applicable qualification, an Accredited Certification Body must inform the Certification Applicant that the notice that personal information is being collected is required for compliance with this principle. Where the Certification Applicant identifies an applicable qualification, an Accredited Certification Body must verify whether the applicable qualification is justified.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement (*evidence provided to meet assessment criteria)***
3. Subject to any qualifications, at the time of collection of personal information (whether directly or through the use of third parties acting for the CA), does the CA indicate the purpose(s) for which personal information is being collected? *MAP TO PART 2 CPRs:* Section 1, CPR 1.7	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify that the Certification Applicant explains to individuals the purposes for which personal information is being collected. The purposes must be communicated orally or in writing, for example on the Certification Applicant's website, such as text on a website link from URL, attached documents, pop-up window, or other. Where the Certification Applicant answers **NO** and does not identify an applicable qualification, an Accredited Certification Body must inform the Certification Applicant of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Certification Applicant identifies an applicable qualification, an Accredited Certification Body must verify whether the applicable qualification is justified.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement (*evidence provided to meet assessment criteria)***
4. Subject to any qualifications, at the time of collection of personal information, does the CA notify individuals that their personal information may be shared with third parties? *MAP TO PART 2 CPRs:* Section 1, CPR 1.1, 1.3	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify that the Certification Applicant provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes. Where the Certification Applicant answers **NO** and does not identify an applicable qualification, an Accredited Certification Body must inform the Certification Applicant to provide notice to individuals that the personal information collected may be shared with third parties. Where the Certification Applicant identifies an applicable qualification, an Accredited Certification Body must determine whether the applicable qualification is justified.	

SECTION 2: COLLECTION LIMITATION

Assessment Purpose - *Ensuring relevant that controls are applied where the Certification Applicant wishes to use, operate, provide, offer or otherwise make available for commercial use a System to engage in High Risk Processing Activities, i.e., that collection of information and is limited to the specific purposes stated at the time of collection. The collection of the information should be relevant to such purposes, and proportionality to the fulfilment of such purposes may be a factor in determining what is relevant. In all instances, collection methods must be lawful and fair.*

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
5. How will the System / the CA obtain personal information: 5.a) Directly from the individual? 5.b) From third parties collecting for the CA? 5.c) Other If YES to any of the above, please describe. *MAP TO PART 2 CPRs:* Section 1, CPR 1.3, 1.4	An Accredited Certification Body must verify that the Certification Applicant indicates from whom they obtain personal information. Where the Certification Applicant answers **YES** to any of these sub- parts, an Accredited Certification Body must verify the Certification Applicant's practices in this regard. There should be at least one 'yes' answer to these three questions. If not, an Accredited Certification Body must inform the Certification Applicant that it has incorrectly completed the questionnaire.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
6. Does the CA / System limit its personal information collection (whether directly or through the use of third parties acting for the CA) to information that is relevant to fulfil the purpose(s) for which it is collected or other compatible or related purposes? *MAP TO PART 2 CPRs:* Section 1, CPR 1.3, 1.4	Where the Certification Applicant answers **YES** and indicates it only collects personal information which is relevant to the identified collection purpose or other compatible or related purposes, an Accredited Certification Body must require the Certification Applicant to identify: • Each type of data collected • The corresponding stated purpose of collection for each; and • All uses that apply to each type of data • An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection Using the above, an Accredited Certification Body will verify that the applicant limits the amount and type of personal information to that which is relevant to fulfil the stated purposes Where the Certification Applicant answers **NO**, an Accredited Certification Body must inform the Certification Applicant that it must limit the use of collected personal information to those uses that are relevant to fulfilling the purpose(s) for which it is collected.	

7. Does the CA / System 7(a) Specifically, where the System allows the CA / System to collect information *directly* from a data subject and intends to Process Personal Data in a manner that will restrict or prevent the Data Subject from exercising his rights to request rectification or erasure of Personal Data in accordance with Article 33 of the Law, or to object to the Processing of the Personal Data in accordance with Article 34, has it: (i) included a clear and explicit explanation of the expected impact on such rights; and (ii) satisfied itself that the Data Subject understands and acknowledges the extent of any such restrictions in accordance with Article 29(1)(h)(ix)? 7(b) Specifically, where the System allows the CA / System to collect information *directly* from a data subject, does the notice about the System include a comprehensive, true and plain description of: (i) the human-defined purposes for which Personal Data is Processed by the System; (ii) all human-defined principles on the basis of which, and all human-defined limits within which, the System is capable of itself defining further purposes for Processing of Personal Data; (iii) the output that the System produces on the basis of such Processing and the manner in which such output is used; (iv) the principles on the basis of which the System has been developed and designed to operate, including a description of any safeguards built into the System by design to ensure compliance of the Processing of Personal Data by the System with the Law and Regulation 10; and (v) the codes, certifications or principles upon which the System is designed or developed, which may include those set out in Regulation 10.2.2(b)	Where the Certification Applicant answers **YES,** an Accredited Certification Body must require the Certification Applicant to certify that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such personal information and that it is collecting information by fair means, without deception. Where the Certification Applicant Answers **NO**, an Accredited Certification Body must inform that Certification Applicant that lawful and fair procedures are required for compliance with this principle. *MAP TO PART 2 CPRs:* Section 1, CPR 1.3, 1.4	

SECTION 3: USES OF PERSONAL INFORMATION

Assessment Purpose - *Ensuring that the use of personal information, particularly where the Certification Applicant wants to use, operate, provide, offer or otherwise make available for commercial use a System to engage in High Risk Processing Activities, is limited to fulfilling the specific purposes of collection and other compatible or related purposes. This section covers use, transfer and disclosure of personal information. Application of this assessment purpose requires consideration of the nature of the information, the context of collection and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" could extend, for example, to matters such as the creation and use of a centralised database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or, the use of information collected by an applicant for the purpose of granting credit for the subsequent purpose of collecting debt owed to that applicant.*

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
8. Does the CA / System limit the use of the personal information collected (whether directly or through the use of third parties acting for the CA) as identified in the relevant Privacy Statement and/or in the notice provided at the time of collection, to those purposes for which the information was collected or for other compatible or related purposes? If necessary, please provide a description in the space provided. *MAP TO PART 2 CPRs:* Section 1, CPR 1.3, 1.4	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify the existence of written policies and procedures to ensure that] all covered personal information collected either directly or indirectly through an agent is done so in accordance with the purposes for which the information was collected as identified in the Certification Applicant's Privacy Statement(s) in effect at the time of collection or for other compatible or related purposes. Where the Certification Applicant Answers **NO**, an Accredited Certification Body must consider answers to Question 9 below.	

9. If NO, does the CA use the personal information that is collected for unrelated purposes under one of the following circumstances? Please describe. 9.a) Based on express consent of the individual? 9.b) Compelled by applicable laws? *MAP TO PART 2 CPRs:* Section 1, CPR 1.3, 1.4	Where the Certification Applicant answers **NO** to question 8, the Certification Applicant must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the applicant selects 9a, an Accredited Certification Body must require the Certification Applicant to provide a description of how such consent was obtained, and an Accredited Certification Body must verify that the Certification Applicant's use of the personal information is based on express consent of the individual (9.a), such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Certification Applicant answers 9.a, an Accredited Certification Body must require the Certification Applicant to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below. Where the Certification Applicant selects 9.b, an Accredited Certification Body must require the Certification Applicant to provide a description of how the collected personal information may be shared, used or disclosed as compelled by law. Where the Certification Applicant does not answer 9.a or 9.b, an Accredited Certification Body must inform the Certification Applicant that limiting the use of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this assessment purpose.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
10. Does the CA / System disclose the personal information that is collected (whether directly or through the use of third parties acting for the CA) to other Controllers? If YES, please describe. *MAP TO PART 2 CPRs:* Section 1, CPR 1.3, 1.4	Where the Certification Applicant answers **YES** in questions 10 and 11, an Accredited Certification Body must verify that if personal information is disclosed to other Controllers or transferred to processors, such disclosure and/or transfer must be undertaken to fulfil the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual, or compelled by law. Also, an Accredited Certification Body must require the Certification Applicant to identify: 1) each type of data disclosed or transferred; 2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfils the identified purpose (e.g. order fulfilment etc.). Using the above, an Accredited Certification Body must verify that the Certification Applicant's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or related purposes.	
11. Does the CA / System transfer personal information to Processors? If YES, please describe. *MAP TO PART 2 CPRs:* Section 1, CPR 1.3, 1.4		
12. If the answer to Question 10 or Question 11 is YES, is the disclosure and/or transfer undertaken to fulfil the original purpose of collection or another compatible or related purpose? If YES, please describe. *MAP TO PART 2 CPRs:* Section 1, CPR 1.3, 1.4		

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
13. If the answer to Question 12 is NO or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances? 13.a) Based on express consent of the individual? 13.b) Necessary to provide a service or product requested by the individual? 13.c) Compelled by applicable laws or judicial orders? *MAP TO PART 2 CPRs:* Section 1, CPR 1.3, 1.4	Where applicant answers **NO** to question 13, the Certification Applicant must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes. Where the Certification Applicant answers **YES** to 13.a, an Accredited Certification Body must require the Certification Applicant to provide a description of how individual's provide consent to having their personal information disclosed and/or transferred for an unrelated use. Where the Certification Applicant answers **YES** to 13.b, an Accredited Certification Body must require the Certification Applicant to provide a description of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual. An Accredited Certification Body must verify that the disclosure or transfer is necessary to provide a service or product requested by the individual. Where the Certification Applicant answers **YES** to 13.c, an Accredited Certification Body must require the Certification Applicant to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Certification Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Certification Applicant is bound by confidentiality requirements. An Accredited Certification Body must verify the existence and applicability of the legal requirement. Where the Certification Applicant answers **NO** to 13.a, b and c, an Accredited Certification Body must inform the Certification Applicant that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this assessment purpose.	

SECTION 4: CHOICE

Assessment Purpose - *Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information, particularly where the Certification Applicant wants to use, operate, provide, offer or otherwise make available for commercial use a System to engage in High Risk Processing Activities. However, this assessment purpose recognises, through the introductory words "where appropriate", that there are certain situations where consent may be clearly provided or, as appropriate, implied, or where it would not be necessary to provide a mechanism to exercise choice. Refer to Appendix C1 for a list of acceptable Qualifications to the provision of choice mechanisms.*

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
14. Subject to the qualifications described below, does the CA provide a mechanism for individuals to exercise choice in relation to the collection of their personal information in general or vis a vis the System being certified? Where YES describe such mechanisms below. *MAP TO PART 2 CPRs:* Section 1, CPR 1.3, 1.4	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify that the Certification Applicant provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to the collection of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) An Accredited Certification Body must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated. Where the Certification Applicant answers **NO**, the Certification Applicant must identify the applicable qualification, and an Accredited Certification Body must verify whether the applicable qualification is justified. Where the Certification Applicant answers **NO** and does not identify an applicable qualification the Accredited Certification Body must inform the Certification Applicant that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.	

15. Subject to the qualifications described below, does the CA provide a mechanism for individuals to exercise choice in relation to the use of their personal information once it is collected, in general or vis a vis the System being certified? Where YES please describe such mechanisms below. *MAP TO PART 2 CPRs:* Section 1, CPR 1.3, 1.4	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify that the Certification Applicant provides a description of mechanisms provided to individuals so that they may exercise choice in relation to the use of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) An Accredited Certification Body must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be used. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent uses of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: • being able to make use of the personal information, when the purpose of such use is not related or compatible to the purpose for which the information was collected, and • Personal information may be disclosed or distributed to third parties, other than Service Providers. Where the Certification Applicant answers **NO**, the Certification Applicant must identify the applicable qualification to the provision of choice and provide a description and an Accredited Certification Body must verify whether the applicable qualification is justified. Where the Certification Applicant answers **NO** and does not identify an acceptable qualification, an Accredited Certification Body must inform the Certification Applicant a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.	

16. Subject to the qualifications described below, does the CA provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information once it is collected, in general or vis a vis the System being certified? Where YES describe such mechanisms below. *MAP TO PART 2 CPRs:* Section 1, CPR 1.3, 1.4	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify that the Certification Applicant provides a description of how individuals may exercise choice in relation to the disclosure of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) An Accredited Certification Body must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be disclosed. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent disclosures of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: • disclosing the personal information to third parties, other than Service Providers, for a purpose that is not related or when an Accredited Certification Body finds that the Certification Applicant's choice mechanism is not displayed in a clear and conspicuous manner, or compatible with that for which the information was collected.] Where the Certification Applicant answers **NO**, the Certification Applicant must identify the applicable qualification to the provision of choice and provide a description and an Accredited Certification Body must verify whether the applicable qualification is justified. Where the Certification Applicant answers **NO** and does not identify an acceptable qualification, an Accredited Certification Body must inform the Certification Applicant that a mechanism for individuals to exercise choice in relation to the disclosure of their personal information must be provided.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
17 When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner? *MAP TO PART 2 CPRs:* Section 1, CPR 1.3, 1.4	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify that the Certification Applicant's choice mechanism is displayed in a clear and conspicuous manner. Where the Certification Applicant answers **NO**, or when an Accredited Certification Body finds that the Certification Applicant's choice mechanism is not displayed in a clear and conspicuous manner, an Accredited Certification Body must inform the Certification Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clear and conspicuous in order to comply with this principle.	
18. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable? *MAP TO PART 2 CPRs:* Section 1, CPR 1.3, 1.4	Where the Certification Applicant answers **YES**, the Accredited Certification Body must verify that the Certification Applicant's choice mechanism is clearly worded and easily understandable. Where the Certification Applicant answers **NO**, and/or when an Accredited Certification Body finds that the Certification Applicant's choice mechanism is not clearly worded and easily understandable, an Accredited Certification Body must inform the Certification Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly worded and easily understandable in order to comply with this principle.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are these choices easily accessible and affordable? Where YES, please describe. *MAP TO PART 2 CPRs:* Section 1, CPR 1.3, 1.4	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify that the Certification Applicant's choice mechanism is easily accessible and affordable. Where the Certification Applicant answers **NO**, or when an Accredited Certification Body finds that the Certification Applicant's choice mechanism is not easily accessible and affordable, an Accredited Certification Body must inform the Certification Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this principle.	
20. What mechanisms are in place so that choices, where appropriate, can be honoured in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Please describe. *MAP TO PART 2 CPRs:* Section 1, CPR 1.3, 1.4	Where the Certification Applicant does have mechanisms in place, an Accredited Certification Body must require the Certification Applicant to provide of the relevant policy or procedures specifying how the preferences expressed through the choice mechanisms (questions 14, 15 and 16) are honoured. Where the Certification Applicant does not have mechanisms in place, the Certification Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accredited Certification Body must verify whether the applicable qualification is justified. Where the Certification Applicant answers **NO** and does not provide an acceptable qualification, an Accredited Certification Body must inform the Certification Applicant that a mechanism to ensure that choices, when offered, can be honoured, must be provided.	

SECTION 5: INTEGRITY OF PERSONAL INFORMATION

Assessment Purpose - *The questions in this section are directed towards ensuring that the Controller maintains the accuracy and completeness of records and keeps them up to date, particularly where the Certification Applicant wishes to use, operate, provide, offer or otherwise make available for commercial use a System to engage in High Risk Processing Activities. This assessment purpose also recognises that these obligations are only required to the extent necessary for the purposes of use.*

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
21. Does the CA / System provide for steps to verify that the personal information collected in general by the CA or vis a vis the System is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, please describe. *MAP TO PART 2 CPRs:* Section 1, CPR 1.7	Where the Certification Applicant answers **YES**, an Accredited Certification Body must require the Certification Applicant to provide the procedures the Certification Applicant has in place to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use. An Accredited Certification Body will verify that reasonable procedures are in place to allow the Certification Applicant to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use. Where the Certification Applicant answers **NO**, an Accredited Certification Body must inform the Certification Applicant that procedures to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
22. Does the CA / System provide for a mechanism for correcting inaccurate, incomplete and outdated personal information to the extent necessary for purposes of use or for monitoring purposes? Please provide a description. *MAP TO PART 2 CPRs:* Section 1, CPR 1.7, 1.8	Where the Certification Applicant answers **YES**, an Accredited Certification Body must require the Certification Applicant to provide the procedures and steps the Certification Applicant has in place for correcting inaccurate, incomplete and outdated personal information, which includes, but is not limited to, procedures which allows individuals to challenge the accuracy of information such as accepting a request for correction from individuals by e-mail, post, phone or fax, through a website, or by some other method. An Accredited Certification Body must verify that this process is in place and operational. Where the Certification Applicant answers **NO**, an Accredited Certification Body must inform the Certification Applicant that procedures/steps to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
23. Where inaccurate, incomplete or out of date information will affect the purposes of use or monitoring and corrections are made to the information subsequent to the transfer of the information, does the CA or System communicate the corrections to Processors, agents, or other service providers to whom the personal information was transferred? If YES, please describe. *MAP TO PART 2 CPRs:* Section 1, CPR 1.7, 1.8	Where the Certification Applicant answers **YES**, an Accredited Certification Body must require the Certification Applicant to provide the procedures the Certification Applicant has in place to communicate corrections to Processors, agent, or other service providers to whom the personal information was transferred and the accompanying procedures to ensure that the corrections are also made by the processors, agents or other service providers acting on the Certification Applicant's behalf. An Accredited Certification Body must verify that these procedures are in place and operational, and that they effectively ensure that corrections are made by the processors, agents or other service providers acting on the Certification Applicant's behalf. Where the Certification Applicant answers **NO**, an Accredited Certification Body must inform the Certification Applicant that procedures to communicate corrections to Processors, agent, or other service providers to whom the personal information was transferred, are required for compliance with this principle.	

24. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, does the CA or System communicate the corrections to other third parties to whom the personal information was disclosed? If YES, please describe. *MAP TO PART 2 CPRs:* Section 1, CPR 1.7, 1.8	Where the Certification Applicant answers **YES**, an Accredited Certification Body must require the Certification Applicant to provide the procedures the Certification Applicant has in place to communicate corrections to other third parties, to whom personal information was disclosed. An Accredited Certification Body must verify that these procedures are in place and operational. Where the Certification Applicant answers **NO**, an Accredited Certification Body must inform the Certification Applicant that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this principle.	
25. Do the CA require Processors, agents, or other service providers acting for the CA to inform it when they become aware of information that is inaccurate, incomplete, or out-of-date? *MAP TO PART 2 CPRs:* Section 1, CPR 1.7, 1.8	Where the Certification Applicant answers **YES**, an Accredited Certification Body must require the Certification Applicant to provide the procedures the Certification Applicant has in place to receive corrections from Processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure that Processors, agents, or other service providers to whom personal information was transferred inform the Certification Applicant about any personal information known to be inaccurate incomplete, or outdated. An Accredited Certification Body will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being made by the Certification Applicant and by the processors, agents or other service providers. Where the Certification Applicant answers **NO**, an Accredited Certification Body must inform the Certification Applicant that procedures to receive corrections from Processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this principle.	

SECTION 6: SECURITY SAFEGUARDS

Assessment Purpose - *The questions in this section are directed towards ensuring that when individuals entrust their information to the Certification Applicant's for use in System(s), that the Certification Applicant will implement reasonable security safeguards to protect individuals' information from loss, unauthorised access or disclosure, or other misuses.*

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
26. Has the CA implemented an information security policy? *MAP TO PART 2 CPRs:* Section 1, CPR 1.6 Section 2, CPR 2.1	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify the existence of this written policy. Where the Certification Applicant answers **NO**, an Accredited Certification Body must inform the Certification Applicant that the implementation of a written information security policy is required for compliance with this principle.	
27. Describe the physical, technical and administrative safeguards that have been implemented to protect personal information against risks such as loss or unauthorised access, destruction, use, modification or disclosure of information or other misuses? *MAP TO PART 2 CPRs:* Section 1, CPR 1.6 Section 2, CPR 2.1, 2.2	Where the Certification Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, an Accredited Certification Body must verify the existence of such safeguards, which may include: • Authentication and access control (e.g. password protections) • Encryption • Boundary protection (e.g. firewalls, intrusion detection) • Audit logging • Monitoring (e.g. external and internal audits, vulnerability scans) • Other (specify) The Certification Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Certification Applicant's size and complexity, the nature and scope of	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
	its activities, and the sensitivity of the personal information and/or Third-Party personal information it collects, in order to protect that information from leakage, loss or unauthorised use, alteration, disclosure, distribution, or access. Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held. The Certification Applicant must take reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorised access, destruction, use, modification or disclosure or other misuses of the information. The Certification Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Certification Applicant indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, an Accredited Certification Body must inform the Certification Applicant that the implementation of such safeguards is required for compliance with this principle.	
28. Describe how the safeguards identified in response to question 27 are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held. *MAP TO PART 2 CPRs:* Section 1, CPR 1.6 Section 2, CPR 2.1, 2.2	Where the Certification Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, an Accredited Certification Body must verify that these safeguards are proportional to the risks identified. The Certification Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Certification Applicant's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a third party) it gathers, in order to protect that information from unauthorised leakage, loss, use, alteration, disclosure, distribution, or access.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
29. Describe how relevant employees are made aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight). *MAP TO PART 2 CPRs:* Section 1, CPR 1.6 Section 2, CPR 2.1, 2.2	An Accredited Certification Body must verify that the Certification Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include: • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other (specify) Where the Certification Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, an Accredited Certification Body has to inform the Certification Applicant that the existence of such procedures is required for compliance with this principle.	
30. Has the CA implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through: 30.a) Employee training and management or other safeguards? 30.b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal? 30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures? 30.d) Physical security?	Where the Certification Applicant answers **YES** (to questions 30.a to 30.d), an Accredited Certification Body has to verify the existence of each of the safeguards. The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Certification Applicant must employ suitable and reasonable means, such as encryption, to protect all personal information. Where the Certification Applicant answers **NO** (to questions 30.a to 30.d), an Accredited Certification Body must inform the Certification Applicant that the existence of safeguards on each category is required for compliance with this principle.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
MAP TO PART 2 CPRs: Section 1, CPR 1.6 Section 2, CPR 2.1, 2.2		
31. Has the CA implemented a policy for secure disposal of personal information?	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify the implementation of a policy for the secure disposal of personal information. Where the Certification Applicant answers **NO**, an Accredited Certification Body must inform Certification Applicant that the existence of a policy for the secure disposal of personal information is required for compliance with this principle.	
32. Has the CA implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures? *MAP TO PART 2 CPRs:* Section 1, CPR 1.6 Section 2, CPR 2.1, 2.2	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures. Where the Certification Applicant answers **NO,** an Accredited Certification Body must inform the Certification Applicant that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this principle.	
33. Does the CA / System have processes in place to test the effectiveness of the safeguards referred to above in question 32? Please describe. *MAP TO PART 2 CPRs:* Section 2, CPR 2.1, 2.2, 2.3	An Accredited Certification Body must verify that such tests are undertaken at appropriate intervals, and that the Certification Applicant adjusts their security safeguards to reflect the results of these tests.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
34. Does the CA conduct risk assessments or third-party certifications to enhance safeguards and security of the System? Please describe below. *MAP TO PART 2 CPRs:* Section 2, CPR 2.1, 2.2, 2.3 Section 3, CPR 3.2	An Accredited Certification Body must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Certification Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Certification Applicant and if audits are carried out, an Accredited Certification Body must verify whether recommendations made in the audits are implemented.	
35. In accordance with relevant laws, regulations or policies, does the CA require processors, agents, contractors, or other service providers to whom it transfers personal information to protect against loss, or unauthorised access, destruction, use, modification or disclosure or other misuses of the information by: 35.a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided? 35.b) Notifying the CA promptly when they become aware of an occurrence of breach of the privacy or security of the personal information of the CA's customers? 35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach? *MAP TO PART 2 CPRs:* Section 2, CPR 2.1, 2.4 Section 3, CPR 3.2	An Accredited Certification Body must verify that the Certification Applicant has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom personal information is transferred, to protect against leakage, loss or unauthorised access, destruction, use, modification or disclosure or other misuses of the information. The Certification Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.	

SECTION 7: ACCESS AND CORRECTION

Assessment Purpose - *The questions in this section are directed towards ensuring that individuals are able to access and correct their information particularly where the Certification Applicant wants to use, operate, provide, offer or otherwise make available for commercial use a System that processes such information to engage in High Risk Processing Activities. This section includes specific conditions for what would be considered reasonable in the provision of access. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access. The details of the procedures whereby the ability to access and correct information is provided may differ depending on the nature of the information and other interests, which is why, in certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records.*

The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. While a Certification Applicant or its System should always make good faith efforts to provide access, in some situations, it may be necessary to deny claims for access and correction. When a CA or the System denies a request for access, for the reasons specified herein, provide the requesting individual with an explanation as to the reason for making that determination and information on how to challenge that denial. The CA would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order. Refer to Appendix C1 for a list of acceptable Qualifications to the provision of access and correction mechanisms.

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
36. Upon request, does the CA provide evidence or other confirmation of whether or not it holds personal information about the requesting individual? Please describe. *MAP TO PART 2 CPRs:* Section 1, CPR 1.1 to 1.4	Where the Certification Applicant answers YES, an Accredited Certification Body must verify that the Certification Applicant has procedures in place to respond to such requests. The Certification Applicant must grant access to any individual, to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity. The Certification Applicant's processes or mechanisms for access by individuals to personal information must be reasonable having regard to the manner of request and the nature of the personal information. The personal information must be provided to individuals in an easily comprehensible way. The Certification Applicant must provide the individual with a time frame indicating when the requested access will be granted. Where the Certification Applicant answers **NO** and does not identify an applicable qualification, an Accredited Certification	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
	Body must inform the Certification Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Certification Applicant identifies an applicable qualification, an Accredited Certification Body must verify whether the applicable qualification is justified.	
37. Upon request, does the CA provide individuals access to the personal information that it holds about them? Where YES, please answer questions 37(a) –(e) and describe the CA's policies/procedures for receiving and handling access requests. Where NO, please proceed to question 38. Otherwise, please state whether the CA: 37.a) Takes steps to confirm the identity of the individual requesting access? If YES, please describe. 37.b) Provides access within a reasonable time frame following an individual's request for access? If YES, please describe. 37.c) Communicates information in a reasonable manner that is generally understandable (in a legible format)? Please describe. 37.d) Provides information in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc.)? 37.e) Charges a fee for providing access? If YES, please describe what the fee is based on and the methodology for ensuring it is not excessive. *MAP TO PART 2 CPRs:* Section 1, CPR 1.1 to 1.4	Where the Certification Applicant answers YES, an Accredited Certification Body must verify each answer provided. The Certification Applicant must implement reasonable and suitable processes or mechanisms to enable the individuals to access their personal information, such as account or contact information. If the Certification Applicant denies access to personal information, it must explain to the individual why access was denied and provide the appropriate contact information for challenging the denial of access where appropriate. Where the Certification Applicant answers **NO** and does not identify an applicable qualification, an Accredited Certification Body must inform the Certification Applicant that it may be required to permit access by individuals to their personal information. Where the Certification Applicant identifies an applicable qualification, an Accredited Certification Body must verify whether the applicable qualification is justified.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
38. Does the CA permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe CA's policies/procedures in this regard below and answer questions 38 (a), (b), (c), (d) and (e). 38.a) Access and correction mechanisms are presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary. 38.b) If an individual demonstrates that personal information about them is incomplete or incorrect, does the CA make the requested correction, addition, or where appropriate, deletion? 38.c) Are such corrections or deletions made within a reasonable time frame following an individual's request for correction or deletion? 38.d) Does the individual receive a copy of the corrected personal information or provide confirmation that the data has been corrected or deleted? 38.e) If access or correction is refused, does the CA provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction? *MAP TO PART 2 CPRs:* Section 1, CPR 1.1 to 1.4	Where the Certification Applicant answers YES to questions 38.a, an Accredited Certification Body must verify that such policies are available and understandable in the primarily targeted economy. If the Certification Applicant denies correction to the individual's personal information, it must explain to the individual why the correction request was denied and provide the appropriate contact information for challenging the denial of correction where appropriate. All access and correction mechanisms must be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting individual. Where the Certification Applicant answers NO to questions 38a-38e and does not identify an applicable qualification, an Accredited Certification Body must inform the Certification Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Certification Applicant identifies an applicable qualification, an Accredited Certification Body must verify whether the applicable qualification is justified.	

SECTION 8: ACCOUNTABILITY, GOVERNANCE AND OVERSIGHT

Assessment Purpose - *The questions in this section are directed towards ensuring that the Certification Applicant is accountable for complying with measures that give effect to the other Principles stated above and ensuring governance and oversight of accountability for the System's function and outputs. Additionally, when transferring information, the Certification Applicant should be accountable for ensuring that the recipient will protect the information consistently. Thus, the CA should take reasonable steps to ensure the information is protected, in accordance with these the Law and relevant principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between CA and the third party to whom the information is disclosed, particularly if done so vis a vis the System. In these types of circumstances, the CA may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, the CA would be relieved of any due diligence or consent obligations.*

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
39. What measures does the CA take to ensure compliance with relevant privacy principles and regulations? Please check all that apply and describe. • Internal guidelines or policies (if applicable, describe how implemented) • Contracts • Compliance with applicable industry or sector laws and regulations • Compliance with self- regulatory applicant code and/or rules • Controls to ensure that the Certification Applicant does not engage in Unfair or Deceptive Practices, as set out in Regulation 6.2. • Other (describe) *MAP TO PART 2 CPRs:* Section 3, CPR 3.1, 3.2, 3.3	An Accredited Certification Body must verify that the Certification Applicant indicates the measures it takes to ensure compliance with the relevant privacy principles.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
40. Has the CA appointed an individual(s), such as an Autonomous Systems Officer, to be responsible for overall compliance with Regulation 10 or other applicable laws and regulations? *MAP TO PART 2 CPRs:* Section 3, CPR 3.1, 3.2, 3.3	Where the Certification Applicant answers **YES,** an Accredited Certification Body must verify that the Certification Applicant has designated an employee(s) who is responsible for the Certification Applicant's overall compliance with these Principles. The Certification Applicant must designate an individual or individuals to be responsible for the Certification Applicant's overall compliance with privacy principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable. Where the Certification Applicant answers **NO**, an Accredited Certification Body must inform the Certification Applicant that designation of such an employee(s) is required for compliance with this principle.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
41. Does the CA have procedures in place to receive, investigate and respond to privacy-related complaints or conflicts? Please describe. *MAP TO PART 2 CPRs:* Section 3, CPR 3.1, 3.2, 3.3	Where the Certification Applicant answers **YES,** an Accredited Certification Body must verify that the Certification Applicant has procedures in place to receive, investigate and respond to privacy-related complaints, such as: • A description of how individuals may submit complaints to the Certification Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR • A designated employee(s) to handle complaints related to the Certification Applicant's compliance with the [ ] and/or requests from individuals for access to personal information; AND/OR • A formal complaint-resolution process; AND/OR • Other (must specify). Where the Certification Applicant answers **NO**, an Accredited Certification Body must inform the Certification Applicant that implementation of such procedures is required for compliance with this principle.	
42. Does the CA have procedures in place to ensure individuals receive a timely response to complaints or conflicts? *MAP TO PART 2 CPRs:* Section 3, CPR 3.1, 3.2, 3.3	Where the Certification Applicant answers **YES,** an Accredited Certification Body must verify that the Certification Applicant has procedures in place to ensure individuals receive a timely response to their complaints. Where the Certification Applicant answers **NO**, an Accredited Certification Body must inform the Certification Applicant that implementation of such procedures is required for compliance with this principle.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
43. If YES, does this response include an explanation of remedial action relating to complaint or conflicts? Please Describe. *MAP TO PART 2 CPRs:* Section 3, CPR 3.1, 3.2, 3.3	An Accredited Certification Body must verify that the Certification Applicant indicates what remedial action is considered.	
44. Does the CA have procedures in place for training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints or conflicts? If YES, please describe. *MAP TO PART 2 CPRs:* Section 3, CPR 3.1, 3.2, 3.3	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify that the Certification Applicant has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints. Where the Certification Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, an Accredited Certification Body must inform the Certification Applicant that the existence of such procedures is required for compliance with this principle.	
45. Does the CA have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information? *MAP TO PART 2 CPRs:* Section 2, 2.4 Section 3, CPR 3.2	Where the Certification Applicant answers **YES, an Accredited** Certification Body must verify that the Certification Applicant has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information, as well as provide the necessary training to employees regarding this subject. Where the Certification Applicant answers **NO**, an Accredited Certification Body must inform the Certification Applicant that such procedures are required for compliance with this principle.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
46. Does the CA have mechanisms in place with processors, agents, contractors, or other service providers pertaining to personal information it processes for the CA, to ensure that any obligations to the individual will be met (check all that apply)? • Internal guidelines or policies (if applicable, describe how implemented) • Contracts • Compliance with applicable industry or sector laws and regulations • Compliance with self- regulatory applicant code and/or rules • Controls to ensure that the Certification Applicant does not engage in Unfair or Deceptive Practices, as set out in Regulation 6.2. • Other (describe) *MAP TO PART 2 CPRs:* Section 2, 2.4 Section 3, CPR 3.1, 3.2, 3.3	Where the Certification Applicant answers **YES, an Accredited** Certification Body must verify the existence of each type of agreement described. Where the Certification Applicant answers **NO**, an Accredited Certification Body must inform the Certification Applicant that implementation of such agreements is required for compliance with this principle.	

47. Do these arrangements or agreements generally require that processors, agents, contractors or other service providers: • [Abide by [ ] -compliant privacy policies and practices as stated in the CA's Privacy Statement?] ——— • Implement privacy practices that are substantially similar to the CA's policies or privacy practices as stated in the Privacy Statement? • Follow instructions provided by the CA relating to the manner in which personal information must be handled? • Impose restrictions on subcontracting unless with the CA's consent? • Notify the Certification Applicant in the case of a breach of the personal information of the Certification Applicant's customers? • Other (describe) *MAP TO PART 2 CPRs:* Section 2, 2.4 Section 3, CPR 3.1, 3.2, 3.3	An Accredited Certification Body must verify that the Certification Applicant makes use of appropriate methods to ensure their obligations are met.	

Question (*to be answered by the Certification Applicant*)	**Assessment Criteria (*to be verified by an Accredited Certification Body*)**	**Relevant Program Requirement *(evidence provided to meet assessment criteria)***
48. Does the CA require Processors, agents, contractors or other service providers to provide it with self-assessments to ensure compliance with its instructions and/or agreements/contracts? If YES, please describe. Section 2, 2.4 Section 3, CPR 3.1, 3.2, 3.3 Section 4	An Accredited Certification Body must verify the existence of such self-assessments.	
49. Does the CA carry out regular spot checking or monitoring of Processors, agents, contractors or other service providers to ensure compliance with its instructions and/or agreements/contracts? If YES, please describe. *MAP TO PART 2 CPRs:* Section 2, 2.4 Section 3, CPR 3.1, 3.2, 3.3 Section 4	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify the existence of the Certification Applicant's procedures such as spot checking or monitoring mechanisms. Where the Certification Applicant answers **NO**, an Accredited Certification Body must require the Certification Applicant to describe why it does not make use of such spot checking or monitoring mechanisms.	
50. Does the CA disclose personal information to other recipient **persons or organisations** in situations where due diligence and reasonable steps to ensure compliance by the recipient as described above is impractical or impossible? *MAP TO PART 2 CPRs:* Section 2, 2.4 Section 3, CPR 3.1, 3.2, 3.3 Section 4	If **YES**, an Accredited Certification Body must ask the Certification Applicant to explain: (1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and (2) the other means used by the Certification Applicant for ensuring that the information, nevertheless, is protected consistent with relevant privacy principles. Where the Certification Applicant relies on an individual's consent, the Certification Applicant must explain to the satisfaction of an Accredited Certification Body the nature of the consent and how it was obtained.	

SECTION 9: TRANSPARENCY AND DUE DILIGENCE IN AUTONOMOUS SYSTEMS DESIGN

Assessment Purpose - *The questions in this section are directed towards ensuring that the Certification Applicant's System design is transparent, such that evidentiary requirements can be met upon request by any relevant person in accordance with Regulation 10.2.2 (c – f), Regulation 10.3.1 and Regulation 10.3.2. Certification Applicant should note that Information provided in accordance with Regulation 10.2.2(c), 10.2.2(d), 10.2.2(e) or 10.2.2(f) may be redacted or summarised, as reasonably determined by the Certification Applicant or relevant party, solely to the minimum extent necessary to protect their intellectual property rights in, or comply with restrictions under applicable laws, in respect of, the System or any raw data used to train the System, provided that the Certification Applicant or relevant party undertaking the summary or redacting (as applicable) must provide to the Commissioner, upon request, the full and unredacted underlying information, and implement any revisions to the summary or redactions that are required by the Commissioner. The Certification Applicant or relevant party may consult with the Commissioner regarding any relevant evidentiary requests or directions at any time.*

Question ***(to be answered by the Certification Applicant)***	**Assessment Criteria** ***(to be verified by an Accredited Certification Body)***	**Relevant Program Requirement** ***(evidence provided to meet assessment criteria)***
51. Has the CA designed the System such that evidence will be provided upon request by any affected party, of the System's compliance with any applicable audit and/or certification requirements that may be established by the Commissioner from time to time? *MAP TO PART 2 CPRs:* Section 1 – all CPRs	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify the existence of the Certification Applicant's procedures for technology design of the System and ability to provide evidence of privacy by design. Where the Certification Applicant answers NO, an Accredited Certification Body must require the Certification Applicant to describe why it does comply with Regulation 10.2.2(c).	
52. Has the CA designed the System such that evidence will be provided upon request by any affected party, of any algorithm(s) that causes the System to seek human intervention when Processing of Personal Data by the System may result in an unfair or discriminatory impact on a Data Subject, as well as a risk and / or impact assessment of the risk that Processing by the System of information made available to the System may result in unjust bias or High Risk Processing? *MAP TO PART 2 CPRs:* Section 1 – all CPRs	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify the existence of the Certification Applicant's procedures for technology design of the System and ability to provide evidence of privacy by design. Where the Certification Applicant answers NO, an Accredited Certification Body must require the Certification Applicant to describe why it does comply with Regulation 10.2.2(d).	

Question ***(to be answered by the Certification Applicant)***	**Assessment Criteria** ***(to be verified by an Accredited Certification Body)***	**Relevant Program Requirement** ***(evidence provided to meet assessment criteria)***
53. Has the CA designed the System such that evidence will be provided upon request by any affected party, of an algorithm or algorithms that cause the Systems to seek human intervention in the event any Personal Data Processed by the System must be accessed by, or on behalf of, competent government authorities, including law enforcement, for the purposes of prevention or prosecution of alleged or confirmed criminal offenses, as well as a risk and impact assessment in that respect? *MAP TO PART 2 CPRs:* Section 1 – all CPRs	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify the existence of the Certification Applicant's procedures for technology design of the System and ability to provide evidence of privacy by design. Where the Certification Applicant answers NO, an Accredited Certification Body must require the Certification Applicant to describe why it does comply with Regulation 10.2.2(e).	
54. Has the CA designed the System such that evidence will be provided upon request by any affected party, of an algorithm or algorithms that instruct the Systems to seek human intervention in the event any Processing of Personal Data by the System may result in non-compliance with Regulation 9, as well as conducting a risk and impact assessment in that respect? *MAP TO PART 2 CPRs:* Section 1 – all CPRs	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify the existence of the Certification Applicant's procedures for technology design of the System and ability to provide evidence of privacy by design. Where the Certification Applicant answers NO, an Accredited Certification Body must require the Certification Applicant to describe why it does comply with Regulation 10.2.2(f).	
55. Has the CA designed the System that will be utilised in products, services, or other use cases that may impact a Data Subject, negatively or positively, is designed in accordance with the following concepts: (a) Ethical: algorithmic decisions and the associated data lineage of a System should be unbiased and mitigated. This principle is closely linked with the principles of fairness and transparency. (b) Fairness: Systems should be designed to treat all individuals equally and fairly, regardless of race,	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify the existence of the Certification Applicant's procedures for technology design of the System and ability to provide evidence of such concepts. Where the Certification Applicant answers NO, an Accredited Certification Body must require the Certification Applicant to describe why it does comply with Regulation 10.3.1.	

Question ***(to be answered by the Certification Applicant)***	**Assessment Criteria** ***(to be verified by an Accredited Certification Body)***	**Relevant Program Requirement** ***(evidence provided to meet assessment criteria)***
gender, or other specifically subjective factors. Additionally, Systems should be designed to avoid potential biases, including unjust bias, or where possible, mitigate bias that could lead to unfair outcomes. (c) Transparent: a System must ensure that Processing of Personal Data is transparent and fair to Data Subjects and other stakeholders in non-technical terms, with appropriate supporting evidence. (d) Secure: a System must keep Personal Data protected and kept confidential and prevent data breaches which could cause reputational, psychological, financial, professional or other types of harm. (e) Accountability: a System must have mechanisms in place to ensure responsibility and accountability for enabling its Systems and outcomes. Such mechanisms may include internal governance and control frameworks in place for monitoring the System, processes and projects regularly or external organisation auditing processes regularly, enabling the assessment of algorithms, data and design processes. *MAP TO PART 2 CPRs:* Section 1 – all CPRs		
56. Has the CA designed the System to ensure that where it wishes to use, operate, provide, offer or otherwise make available for commercial use it to Process Personal Data (or receive the benefit of, or output from, the operation of such System), it:	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify the existence of the Certification Applicant's procedures for technology design of the System and ability to provide evidence of due diligence with respect to security and privacy by design.	

Question ***(to be answered by the Certification Applicant)***	**Assessment Criteria** ***(to be verified by an Accredited Certification Body)***	**Relevant Program Requirement** ***(evidence provided to meet assessment criteria)***
(a) is capable of Processing Personal Data only for purposes that are human-defined or human-approved, or are defined by the System itself solely on the basis of human-defined principles and solely within the limits of human-defined constraints; and (b) is designed in compliance with Regulation 10.3.1 and complies with any other applicable audit and certification requirements that may be established by the Commissioner from time to time. *MAP TO PART 2 CPRs:* Section 1 – all CPRs	Where the Certification Applicant answers NO, an Accredited Certification Body must require the Certification Applicant to describe why it does comply with Regulation 10.3.2.	
57. Has the CA appointed an Autonomous Systems Officer (ASO), who will have the same or substantially similar competencies, status, role and task of a DPO as set out in Article 17 and Article 18 of the Law? *MAP TO PART 2 CPRs:* Section 1 – all CPRs	Where the Certification Applicant answers **YES**, an Accredited Certification Body must verify the existence of the Certification Applicant's procedures for and appointment of the ASO. Where the Certification Applicant answers NO, an Accredited Certification Body must require the Certification Applicant to assess and determine whether it engages in HRP, if it must appoint a Data Protection Officer, or provide a reasonable explanation about why it does comply with Regulation 10.3.3(d).	

C1. Certification Program Requirements Conditions of Acceptance and Qualifications

The conditions of acceptance are subjective conclusions to be determined by the Accredited Certification Body through examination of information provided to meet Certification Program Requirements. They should be based largely on the policy objectives set out in Part 2 of the Framework.

1 Obligations of Deployers, Operators and Providers of Systems Regarding Purposes and Principles

Conditions of acceptance:

[Outline here, if any]

Reasons for Rejection:

[Outline here]

Qualifications:

Notice

Where not directly related to the notice requirements for certification of Systems as set out in Regulation 10.3.3, the following may be considered with respect to general notice criteria in Section 1 of the Sample Certification Program Requirements:

a) *Disclosure to a government institution which has made a request for the information with lawful authority*: Certification Applicants do not need to provide notice of disclosure to law enforcement agencies for investigation purposes where the provision of such notice to the individual will likely prejudice the investigation, but may do so:

    i) as best practice on the basis of enhanced due diligence regarding the necessity and proportionality of the request; and

ii) provided that the time to conduct such due diligence does not on balance create harm to individuals or public safety.

b) *Disclosure to a third party pursuant to a lawful form of process*: Certification Applicants do not need to provide notice of disclosure to a third party when such disclosure was requested pursuant to a lawful form of process such as a discovery request made in the course of civil litigation.

c) *For legitimate investigation purposes*: When providing notice would compromise the availability or accuracy of the information and the collection, use and disclosure are reasonable for purposes relating to an internal or external investigation of a violation of a code of conduct, breach of contract or a contravention of domestic law.

d) *Action in the event of an emergency*: Certification Applicants do not need to provide notice in emergency situations that threaten the life, health or security of an individual.

Choice

Where not directly related to the choice requirements for certification of Systems, the following qualifications may be considered with respect to general choice criteria in Section 4 of the Sample Certification Program Requirements:

a) *Third-Party Receipt*: Where personal information is received from a third party, the recipient Certification Applicant does not need to provide a mechanism for individuals to exercise choice in relation to the collection of the information. However, if Certification Applicant engages a third party to collect personal information on its behalf, the Certification Applicant should instruct the collector to provide such choice when collecting the personal information.

b) *Disclosure to a government institution which has made a request for the information with lawful authority*: Certification Applicants do not need to provide a mechanism for individuals to exercise choice in relation to disclosure to law enforcement agencies for investigation purposes where the provision of such mechanism to the individual will likely prejudice the investigation.

c) *Disclosure to a third party pursuant to a lawful form of process*: Certification Applicants do not need to provide a mechanism for individuals to exercise choice in relation to the disclosure to a third party when such disclosure was requested pursuant to a lawful form of process such as a discovery request made in the course of civil litigation.

d) *For legitimate investigation purposes*: When providing a mechanism for individuals to exercise choice would compromise the availability or accuracy of the personal information and its collection, use and disclosure are reasonable for purposes relating to an internal or external investigation of a violation of a code of conduct, breach of contract or a contravention of domestic law.

e) *Action in the event of an emergency*: Certification Applicants do not need to provide a mechanism for individuals to exercise choice in emergency situations that threaten the life, health or security of an individual.

Access and Correction

Although organisations should always make good faith efforts to provide access, there are some situations, described below, in which it may be necessary for organisations to deny or request to reasonably modify access requests. Please identify which, if any, of these situations apply, and specify its application to the processing / System design, with reference to responses provided to the previous questions in Section 7 of the Sample Certification Program Requirements.

a) *Disproportionate Burden:* Certification Applicants do not need to provide access and correction where the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question, as for example when claims for access are repetitious or vexatious by nature.

b) *Protection of Confidential Information*: Certification Applicants do not need to provide access and correction where the information cannot be disclosed due to legal or security reasons or to protect confidential commercial information (i.e. information that the CA has taken steps to protect from disclosure, where such disclosure would facilitate a competitor in the market to use or exploit the information against business interests causing significant financial loss). Where confidential commercial information can be readily separated from other information subject to an access request, the Certification Applicants include in its System design the ability to permit redaction of the confidential commercial information and make available the non-confidential commercial information to the extent that such information constitutes personal information of the individual concerned. Other situations would include those where disclosure of information would benefit a competitor in the marketplace, such as a particular computer or modelling program. Furthermore, a denial of access may also be considered acceptable in situations where, for example providing the information would constitute a violation of laws or would compromise security.

c) *Third Party Risk*: Certification Applicants do not need to provide access and correction where the information privacy of persons other than the individual would be violated. In those instances where a third party's personal information can be severed from the information requested for access or correction, the Certification Applicants must release the information after redaction of the third party's personal information collected from or by the System.

2 Third Parties and Compliance

Conditions of acceptance:

[Outline here, if any]

Reasons for Rejection:

[Outline here]

3 Governance and Oversight

Conditions of acceptance:

[Outline here, if any]

Reasons for Rejection:

[Outline here]

4 Audit Criteria

Conditions of acceptance:

[Outline here, if any]

Reasons for Rejection:

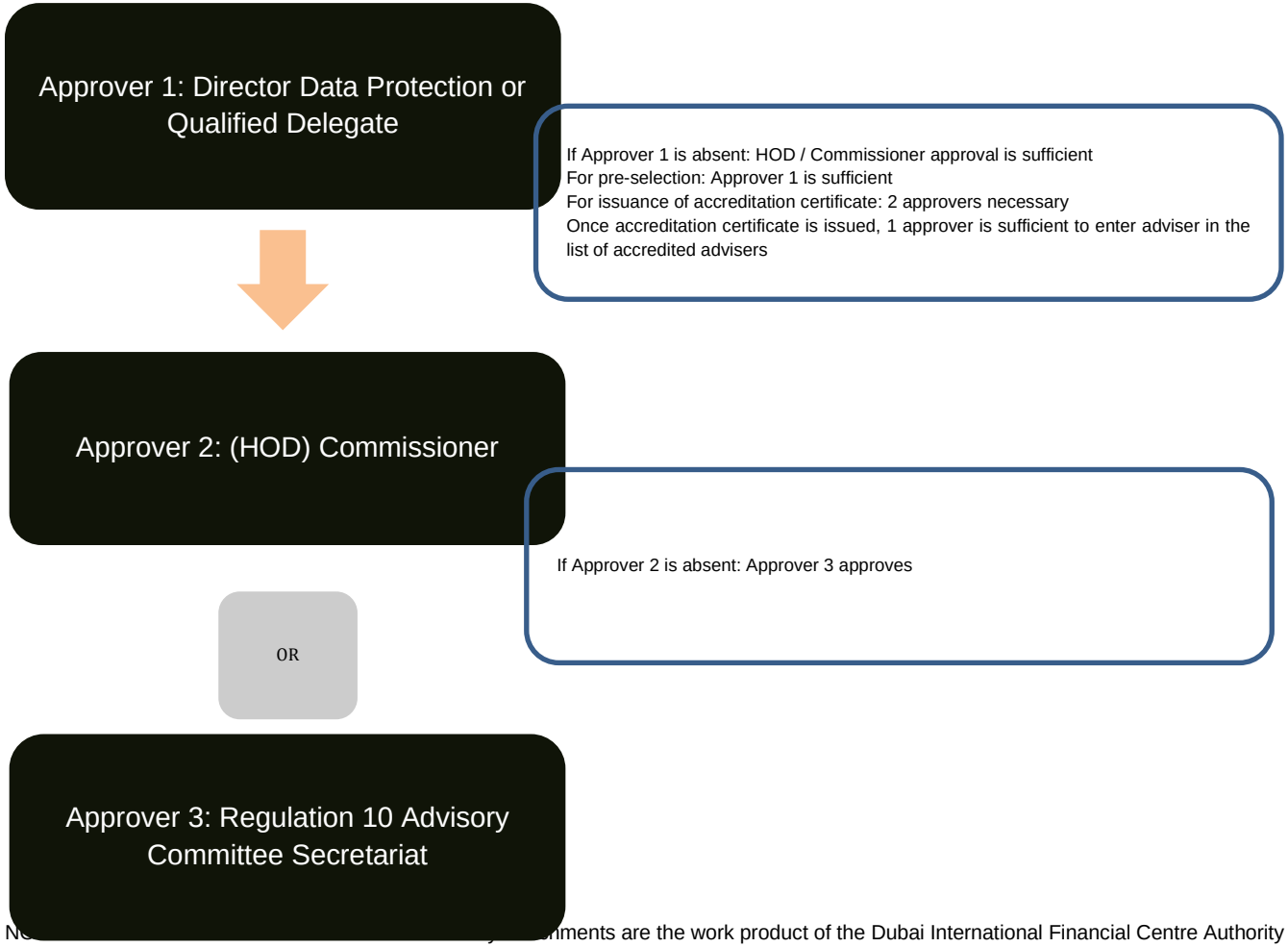
[Outline here]

DIFC

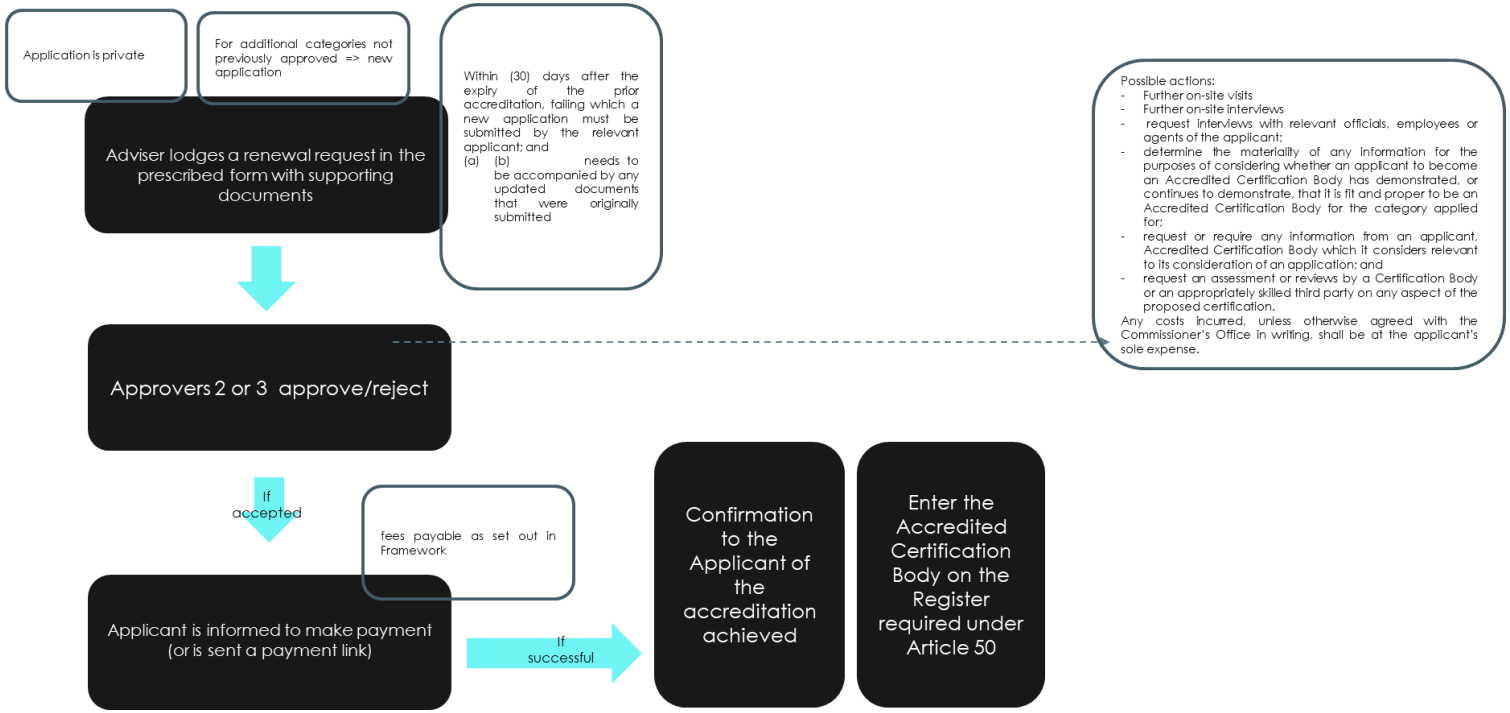
Appendix D – High-level Review and Approvals Workflows

The following workflows are indicative only and may be subject to change.

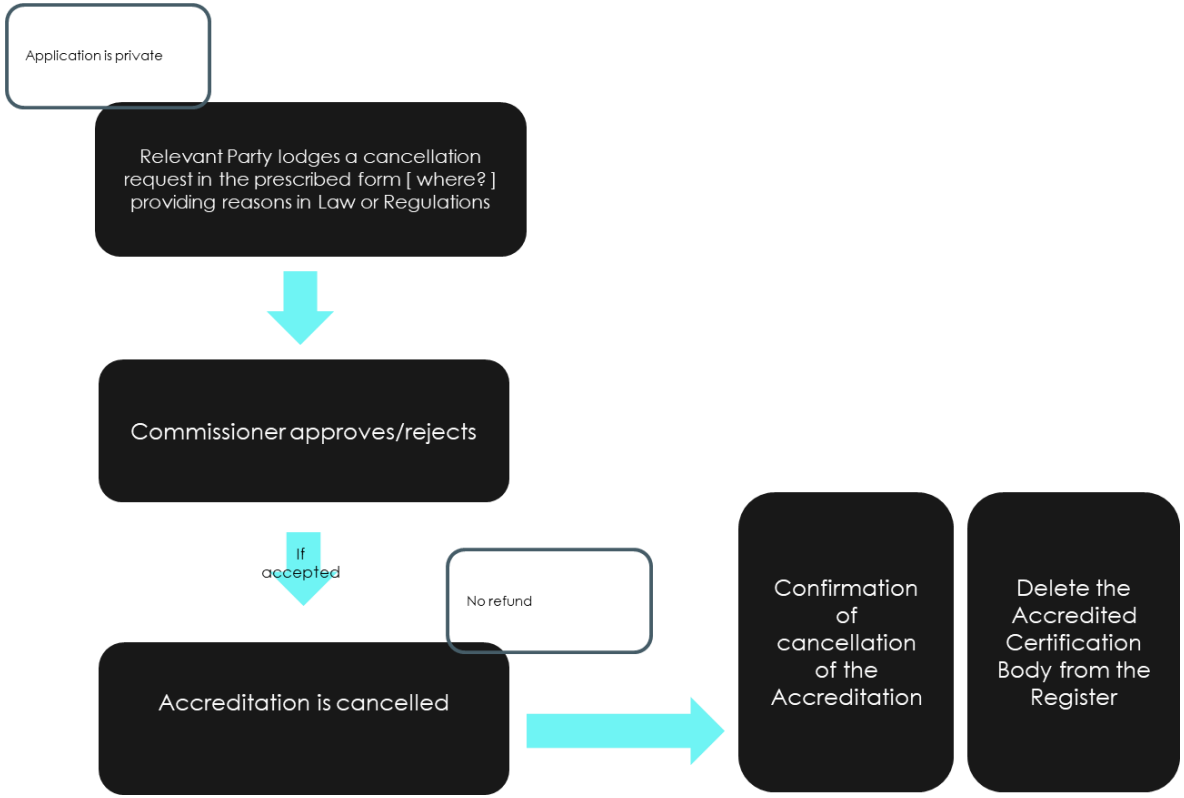
Administrative Approvals Flow for Accredited Certification Body Applications



Accreditation workflow: application renewal



Accreditation workflow: cancellation of application



Note: Relevant Party can be any interested party, including those who have complained that the certification / approval is unfair or deceptive.

Accreditation workflow: revoking an application