1. Data Protection Policy

1.1. Relevant Legislation

1. Data Protection Law (DIFC Law no 5 of 2020)
   https://www.difc.ae/files/6115/9358/6486/Data_Protection_Law_DIFC_Law_No.5_of_2020.pdf

2. Data Protection Regulations
   https://www.difc.ae/files/9315/9358/7756/Data_Protection_Regulations_2020.pdf

3. Comprehensive guides on matters related to Data Protection
   https://www.difc.ae/business/operating/data-protection/guidance/

1.2. Defined terms

Term	Definition
Controller	Any person who alone or jointly with other persons determinates the purposes and means of the Processing of Personal Data.
Data Subject	The identified or Identifiable Natural Person to whom Personal Data relates.
High Risk Processing Activities	Processing of Personal Data where one or more of the following applies: ▸ Processing that includes the adoption of new or different technologies or methods, which creates a materially increased risk to the security or rights of a Data Subject or renders it more difficult for a Data Subject to exercise his rights; ▸ a considerable amount of Personal Data will be Processed (including staff and contractor Personal Data) and where such Processing is likely to result in a high risk to the Data Subject, including due to the sensitivity of the Personal Data or risks relating to the security, integrity or privacy of the Personal Data; ▸ the Processing will involve a systematic and extensive evaluation of personal aspects relating to natural persons, based on automated Processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; or ▸ a material amount of Special Categories of Personal Data is to be Processed
Identifiable Natural Person	A natural living person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his biological, physical, biometric, physiological, mental, genetic, economic, cultural or social identity.

Personal Data	Any information referring to an identified or Identifiable Natural Person.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
Process, Processed, Processes and Processing	Any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage and archiving, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, transfer or otherwise making available, alignment or combination, restricting (meaning the marking of stored Personal Data with the aim of limiting Processing of it in the future), erasure or destruction, but excluding operations or sets of operations performed on Personal Data by: ▸ a natural person in the course of a purely personal or household activity that has no connection to a commercial purpose; or ▸ law enforcement authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security.
Processor	Any person who Processes Personal Data on behalf of the Firm.
Special Categories of Personal Data	Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person.
DPO	A data protection officer appointed by the Firm to independently oversee relevant data protection operations.

1.3. Scope

This Data Protection Policy applies to all Personal Data processed by the Firm and is part of the Firm's approach to comply with the applicable Data Protection provisions. All staff are expected to comply with this policy and failure to comply may lead to disciplinary action for misconduct, including dismissal.

1.4. General requirements for legitimate and lawful processing

The Firm complies with the Data Protection principles set out below.

Principle	Requirement
Lawfulness, fairness and transparency	The Firm ensures that Personal Data is processed lawfully, fairly and in a transparent manner in relation to the Data Subject

Principle	Requirement
Purpose limitation	The Firm ensures that Personal Data is collected and processed for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data minimisation	The Firm ensures that processed Personal Data is all relevant and limited to what is necessary in relation to the purposes for which they are processed.
Accuracy	The Firm ensures that processed Personal Data is all accurate and, where necessary, kept up to date and that reasonable steps are taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
Storage limitation	The Firm ensures that Personal Data is kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed.
Integrity and confidentiality	The Firm ensures that Personal Data is processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

How the Firm complies with these general requirements is documented in this Policy and in the Firm's Privacy Statement.

1.5. Lawfulness of processing

In general, the Firm processes Personal Data where:

- Processing is necessary for the performance of a contract to which a Data Subject is a party, or in order to take steps at the request of a Data Subject prior to entering into such contract;
- Processing is necessary for compliance with applicable laws that the Firm is subject to (e.g. Anti-Money Laundering, Conduct of Business, Common Reporting Standards, FATCA);
- Processing is necessary in order to protect the vital interests of a Data Subject or of another natural person; or
- Processing is necessary for the purpose of legitimate interests pursued by the Firm or a third party to whom the Personal Data has been made available.
- Furthermore, processing is legitimate if it is necessary and proportionate to prevent fraud or to ensure network and information security.

The Firm will seek the Data Subject's written consent to process his/her Personal Data for any other clearly defined purpose (for instance for direct marketing purposes).

1.6. Lawful Processing of Special Categories of Personal Data

The Firm **only** processes Special Categories of Personal Data if one or more of the following applies:

- Processing is necessary for the carrying out the obligation or exercising the specific rights of the Firm or a Data Subject in the context of the Data Subject's employment;
- Processing is necessary to protect the vital interests of a Data Subject;
- Processing relates to Personal Data that has been made public by a Data Subject;
- Processing is necessary for compliance with a specific regulatory requirement to which the Firm is subject, and in such circumstances the Firm provides the Data Subject with clear notice of such processing as soon as reasonably practicable;
- Processing is necessary to comply with regulatory requirements that applies to the Firm in relation to anti-money laundering or counter-terrorist financing obligations or the prevention, detection or prosecution of any crime;
- Processing is required for protecting members of the public against dishonesty, malpractice, incompetence or other improper conduct of persons providing banking, insurance, investment, management consultancy, information technology services, accounting or other services or commercial activities (either in person or indirectly by means of outsourcing), including any resulting financial loss.

The Firm will seek the Data Subject's explicit consent for processing his/her Special Categories of Personal Data for other clearly defined purposes.

1.7. Information to Data Subjects (Privacy Statement)

The Firm has adopted a Privacy Statement by which it provides its Data Subjects with data protection information, in a concise, transparent, intelligible and easily accessible form, using clear and plain language, at the time of collecting the Personal Data to enable the Data Subjects to assess the implications of providing their Personal Data:

- the Firm's identity and contact details;
- the contact details of the DPO, if applicable;
- the purposes of the processing, as well as its lawful basis under the Data Protection Law;
- if the Firm's lawful basis for the Processing is legitimate interests or compliance with any applicable law to which the Firm is subject, the Firm states clearly what those legitimate interests or compliance obligations are;
- the categories of Personal Data relating to the Data Subject that are being processed;
- the recipients or categories of recipients of the Personal Data;
- where applicable, the fact that the Firm intends to transfer Personal Data to a third country or international organisation, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available; and
- any further information in so far as such is necessary, having regard to the specific circumstances in which the Personal Data is collected, to ensure fair and transparent processing in respect of the Data Subject, including:
    - the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
    - the existence of the right to request from the Firm access to and rectification;
    - or erasure of Personal Data or restriction of processing concerning the Data Subject or to object to processing as well as the right to data portability;
    - where the processing is based on the Data Subject's consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of Processing based on consent before its withdrawal;

- the right to lodge a complaint with the Data Protection Commissioner;
- whether the Personal Data is obtained pursuant to a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and the possible consequences of failure to provide such data;
- if applicable, the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the possible outcomes of such processing for the Data Subject;
- whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply;
- whether the Personal Data will be used for direct marketing purposes; and
- if the Firm 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 or to object to the Processing of the Personal Data. In such cases, the Firm:
  - include a clear and explicit explanation of the expected impact on such rights; and
  - satisfy itself that the Data Subject understands and acknowledges the extent of any such restrictions.

Where Personal Data is not obtained from the Data Subject, the Firm shall provide the above information:

- No later than one month from obtaining the Persona Data;
- If the Personal Data is used for communicating with the Data Subject, no later than the first communication
- If a disclosure to a Processor or a third party is envisaged, no later than the time when the Personal Data is first disclosed.

The Firm's Privacy Statement is made available on its website. Data Subjects are directed to this Private Statement using weblinks in the Firm's client communications, forms and agreements.

1.8. Oversight and compliance responsibility

On the basis that the Firm isn't performing High Risk Processing Activities, it isn't required to appoint a DPO. The Firm has clearly allocated responsibility for oversight and compliance with respect to data protection duties and obligations within its organization to its compliance function.

The Firm is required to appoint a Data Protection Officer ("DPO") when it is performing High Risk Processing Activities on a systematic or regulator basis. The Firm's compliance function assesses annually or whenever the Firm's makes fundamental amendments to its business or operating model whether it is performing High Risk Processing Activities.

Where the Firm is required to appoint a DPO, the DPO must undertake an assessment of the Firm's processing activities at least once per year which shall be submitted to the Data Protection Commissioner. This Annual Assessment Report includes a reporting on the processing activities performed by the Firm and indicates whether the Firm intends to perform High Risk Processing Activities in the following annual period. The first submission of the Annual Assessment will be made on the first license renewal date after 1 July 2021.

1.9. Data Protection Impact Assessment (High Risk Processing Activities)

Before undertaking High Risk Processing Activities, the Firm must carry out an assessment of the impact of the proposed processing operations on the protection of Personal Data, considering the rights of the Data Subjects

concerned. Although not mandatory, it is recommended to perform such assessment for any intended processing of Personal Data.

The DPO, where appointed, is responsible for overseeing data protection impact assessments.

A data protection impact assessment contains at least:

- a systematic description of the foreseen processing operations and the purpose(s) of the processing, including, where applicable, the legitimate interest pursued by the Firm;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- identification and consideration of the lawful basis for the processing, including:
    - where legitimate interests are the basis for processing, an analysis and explanation of why the Firm believes the interests or rights of a Data Subject do not override its interests; and
    - where consent is the basis for processing, validation that such consent is validly obtained, consideration of the impact of the withdrawal of consent to such processing and of how the Firm will ensure compliance with the exercise of a Data Subject's right to withdraw consent;
- an assessment of the risks to the rights of Data Subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with the Data Protection Law, considering the rights and legitimate interests of Data Subjects and other concerned persons.

Whenever there is a requirement for the Firm to conduct a data protection impact assessment, it carries out a review to assess if processing is performed in accordance with a data protection impact assessment:

- on a regular basis, proportionate to the extent and type of processing the Firm conducts; or
- when there is a change in the risk related to the processing operations.

Where a data protection impact assessment indicates that despite taking all required measures, the risks to the rights of the Data Subjects remain particularly high, the Firm must consult with the Data Protection Commissioner preferably prior to carrying out a processing activity.

1.10. Accountability

The Firm has established a compliance monitoring program to demonstrate its compliance with the Data Protection Law.

The Firm has implemented appropriate technical and organisational measures to demonstrate that processing is performed in accordance with the Data Protection Law.

The Firm considers:

- the nature, scope, context and purpose of the processing;
- the risks presented by the processing to a relevant Data Subject; and
- prevailing information security good industry practice.

The Firm ensures a level of security:

- appropriate to the risks associated with processing, taking account of any wilful, negligent, accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of or access to Personal Data; and
- against all other unlawful forms of Processing;

The Firm ensures that, by default, only Personal Data necessary for each specific purpose is processed. This obligation applies to the amount and type of Personal Data collected, the extent of the processing, the period of storage and accessibility; and

The Firm reviews and updates such measures where necessary to reflect legal, operational and technical developments.

The Firm has implemented and maintains a data protection policy in writing that is proportionate to the extent and type of processing of Personal Data undertaken; and consistent with the Data Protection Law.

The Firm has registered with the Data Protection Commissioner by filing a notification of processing operations, which is kept up to date through amended notifications.

The Firm's compliance function is responsible for demonstrating and monitoring the Firm's compliance with the principles and requirements mentioned in this section.

1.11. Working with (Sub)- Processors

Where processing is carried out on behalf of the Firm by a Processor, the processing shall be governed by a legally binding written agreement between the Firm and the Processor.

The Firm only enters into agreements with processors that provide enough assurances to implement appropriate technical and organizational measures that ensure the processing meets the data protection requirements and protects the Data Subject's rights. A Processor may not engage another Processor to act as a Sub-processor without the Firm's prior written authorisation. Sub-processing must be documented in a legally binding written agreement between the Processor and Sub-processor.

The agreement must set out the:

- Subject-matter and duration of processing
- Nature and purpose of the processing
- Type of Personal Data and categories of Data Subjects; and
- The Firm's obligations and rights.

Furthermore, the agreement must include commitments that each Processor and Sub-processor (if any) shall:

- Process Personal Data based on documented instructions from the Firm, including sharing of Personal Data in response to a request made by a Requesting Authority, or transfers of Personal Data to a Third Country or an International Organisation, unless required to do so by applicable laws to which the Processor is subject;
- where applicable law applies, inform any relevant counterparty; or where there is a chain of Processors and Sub-processors, ensure that the Firm is notified, unless the applicable law in question prohibits such information being provided on grounds of substantial public interest;
- ensure that persons authorised to process relevant Personal Data are under legally binding written agreements or duties of confidentiality;
- take all required accountability and notification measures;
- assist a relevant counterparty by providing appropriate technical and organisational measures for the fulfilment of the Firm's obligation to respond to requests for exercising the Data Subject's rights, having considered the nature of the processing;
- assist a relevant counterparty in ensuring the Firm's compliance with applicable data protection obligations, considering the nature of processing and the information available to the Processor;

- delete or return all Personal Data to the Firm, at the Firm's option, or make the same available for return to a relevant counterparty after the end of the provision of services relating to processing, and delete existing copies unless applicable law requires storage of the Personal Data;
- make available to the Firm, relevant counterparty or the Data Protection Commissioner (upon request) all necessary information to demonstrate compliance with applicable data protection regulations; and
- permit and provide reasonable assistance with audits, including inspections, conducted by a relevant counterparty; another auditor mandated by a relevant counterparty; or the Data Protection Commissioner.

A Processor or Sub-processor shall immediately inform the Firm or Processor (as applicable) whether, in its opinion, the processing activity infringes the Data Protection Law.

The Firm, the Processor or Sub-Processor, must take steps to ensure that any person acting under its authority that has access to Personal Data, shall not process it except on the instructions of the Firm, unless it is required to do so under applicable law.

1.12. Data Export – Transfer of Personal Data out of the DIFC

Whenever the Firm intends to transfer Personal Data out of the DIFC into other countries, it assesses and documents under what circumstances/conditions such transfer is permitted.

Transfer of Personal Data from the DIFC may only take place if:

- it is to country or international organization that in the opinion of the Data Protection Commissioner ensures an adequate level of data protection (see Table 1 below).
- the Firm or Processor has provided appropriate safeguards and on condition that enforceable Data Subject rights and effective legal remedies for Data Subjects are available. Appropriate safeguards may be provided for by:
    - a legally binding instrument between public authorities;
    - standard data protection clauses as adopted by the Data Protection Commissioner;
    - an approved code of conduct together with binding and enforceable commitments of the Firm or Processor in the third country or the international organisation to apply the appropriate safeguards, including regarding a Data Subject's rights; or
    - an approved certification mechanism together with binding and enforceable commitments of the Firm or Processor in the third country or the international organisation to apply the appropriate safeguards, including regarding Data Subjects' rights.
- One of the below derogations apply:
    - **a Data Subject has explicitly consented to a proposed transfer, after being informed of possible risks of such transfer due to the absence of an adequacy decision or appropriate safeguards;**
    - the transfer is necessary for the performance of a contract between a Data Subject and the Firm or the implementation of pre-contractual measures taken in response to the Data Subject's request;
    - the transfer is necessary for the conclusion or performance of a contract that is in the interest of a Data Subject between the Firm and a third party;
    - the transfer is necessary for reasons of substantial public interest;
    - the transfer is necessary for the establishment, exercise or defence of a legal claim;
    - the transfer is necessary in order to protect the vital interests of a Data Subject or of other persons where a Data Subject is physically or legally incapable of giving consent;
    - the transfer is necessary for compliance with any obligation under applicable law to which the Firm is subject; or made at the reasonable request of a regulator, police or other government agency or competent authority;

- subject to international financial standards, the transfer is necessary to uphold the legitimate interests of the Firm recognised in international financial markets, except where such interests are overridden by the legitimate interests of the Data Subject relating to the Data Subject's situation; or
- the transfer is necessary to comply with applicable anti-money laundering or counterterrorist financing obligations that apply to the Firm or Processor or for the prevention or detection of a crime.

The following third countries ensure in the opinion of the Data Protection Commissioner an adequate level of protection:

Table 1

ADGM	Estonia	Italy	Portugal
Andorra	Faroe Islands	Japan	Romania
Argentina	Finland	Jersey	Slovakia
Austria	France	Latvia	Slovenia
Belgium	Germany	Liechtenstein	Sweden
Bulgaria	Greece	Lithuania	Switzerland
Canada	Guernsey	Luxembourg	United Kingdom
Croatia	Hungary	Netherlands	Uruguay
Cyprus	Iceland	New Zealand	
Czech Republic	Ireland	Norway	
Denmark	Isle of Man	Poland	

1.13. Data sharing with public authorities

Where the Firm receives a request from any public authority over the person or any part of its Group ("a **Requesting Authority**") for the disclosure and transfer of any Personal Data, it:

- exercises reasonable caution and diligence to determine the validity and proportionality of the request, including to ensure that any disclosure of Personal Data in such circumstances is made solely for the purpose of meeting the objectives identified in the request from the Requesting Authority;
- assess the impact of the proposed transfer in light of the potential risks to the rights of any affected Data Subject and, where appropriate, implement measures to minimise such risks, including by redacting or minimising the Personal Data transferred to the extent possible or utilising appropriate technical or other measures to safeguard the transfer; and
- where reasonably practicable, obtain appropriate written and binding assurances from the Requesting Authority that it will respect the rights of Data Subjects and comply with the general data protection in relation to the Processing of Personal Data by the Requesting Authority.

The Firm may disclose or transfer Personal Data to the Requesting Authority where it has taken reasonable steps to satisfy itself that:

- a request by the Requesting Authority is valid and proportionate; and
- the Requesting Authority will respect the rights of Data Subjects in the processing of any Personal Data transferred to it by the Firm.

1.14. Data Subject Rights

The Firm has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under the Data Protection Law. All staff receives training and are aware of the rights of Data Subjects. Staff can identify such a request and know who to send it to. All requests received from Data Subjects must be sent to the [DPO], compliance function and SEO.

Data Subjects can contact the Firm regarding their data protections rights 1) by post (letter addressed to the compliance function), 2) by email or 3) by completing a contact form on the Firm's website.

1.14.1. Right to withdraw consent

Where the basis for processing Personal Data is consent, the Data Subject may withdraw its consent at any time by notifying the Firm. A Data Subject must be informed on this right.

Upon the exercise of a Data Subject's right to withdraw consent, the Firm ceases processing the Personal Data as soon as reasonably practicable (which is within maximum 1 month) and ensures that any Processors do the same.

1.14.2. Right to access, rectification and erasure of Personal Data

1.14.2.1. Right to access

Upon request, a Data Subject has the right to obtain from the Firm without charge and within 1 month of the request:

- confirmation in writing as to whether or not Personal Data relating to him/ her is being processed and information at least as to the purposes of the processing, the categories of Personal Data concerned, and the recipients or categories of recipients to whom the Personal Data are disclosed;
- a copy of the Personal Data undergoing processing in electronic form and of any available information as to its source, including up-to-date information corresponding with the information requirements set out in the Firm Privacy Statement; and
- the rectification of Personal Data unless it is not technically feasible to do so.

1.14.2.2. Right to Erasure

The Data Subject has the right to require the Firm to erase his Personal Data where:

- the processing of the Personal Data is no longer necessary in relation to the purposes for which it was collected;
- a Data Subject has withdrawn consent to the processing where consent was the lawful basis for processing and there is no other lawful basis;
- the processing is unlawful, or the Personal Data is required to be deleted to comply with applicable law to which the Controller is subject; or
- the Data Subject objects to the processing and there are no overriding legitimate grounds for the Firm to continue with the processing.

The Firm shall direct all recipients and Processors to rectify or erase Personal Data where the respective right is properly exercised or to cease processing and return or erase the Personal Data where the right to object is validly exercised.

1.14.3. Right to object to processing

A Data Subject has the right to:

- object at any time on reasonable grounds relating to his situation to processing of Personal Data relating to him where such processing is carried out on the basis that:
  - it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Firm; or
  - it is necessary for the purposes of the legitimate interests, where applicable, of the Firm or of a third party; and
- be informed before Personal Data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object to such disclosures or uses; and
- where Personal Data is processed for direct marketing purposes, object at any time to such processing, including profiling to the extent that it is related to such direct marketing.

1.14.4. Right to restriction of processing

Data Subject has the right to require the Firm to restrict processing to the extent that any of the following circumstances apply:

- the accuracy of the Personal Data is contested by the Data Subject, for a period allowing the Firm to verify the accuracy of the Personal Data;
- the processing is unlawful, and the Data Subject opposes the erasure of the Personal Data and requests the restriction of its use instead;
- the Firm no longer needs the Personal Data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;
- the Data Subject has objected to processing pending verification of whether the legitimate grounds of the Firm override those of the Data Subject.

If the Firm lifts the period of restriction it informs the Data Subject in writing.

1.14.5. Right to data portability

A Data Subject has the right to receive Personal Data that he has provided to the Firm in a structured, commonly used and machine-readable format where the processing is:

- based on the Data Subject's consent or the performance of a contract; and
- carried out by automated means.

The purpose of is to enable ready portability between the Firm and other Controllers if so required by the Data Subject, and the Data Subject has the right to have the Personal Data transmitted directly from the Firm to whom the request is made to any other person, where technically feasible.

1.14.6. Right to object automated individual decision-making, including profiling

A Data Subject has the right to object to any decision based solely on automated processing, including profiling, which produces legal consequences concerning him or other seriously impactful consequences and to require such decision to be reviewed manually.

1.15. Cessation of processing

Where the basis for processing changes, ceases to exist or the Firm is required to cease processing due to the exercise of a Data Subject's rights, the Firm ensures that all Personal Data, including Personal Data held by processors is:

- securely and permanently deleted;
- anonymised so that the data is no longer Personal Data and no Data Subject can be identified from the data including where the data is lost, damaged or accidentally released;
- pseudonymised;
- securely encrypted.

Alternatively, where the Firm is unable to ensure that Personal Data is securely and permanently deleted, anonymised, pseudonymised or securely encrypted, the Personal Data is archived in a manner that ensures the data is "put beyond further use".

"Put beyond further use" means that:

- the Firm and a relevant Processor is unable to use the Personal Data to inform any decision with respect of the Data Subject or in a manner that affects the Data Subject in any way, other than where such Personal Data needs to be cross-checked by automated means solely in order to prevent further Processing of Personal Data related to the Data Subject;
- no party has access to the Personal Data other than the Firm and any relevant Processor;
- Personal Data is protected by appropriate technical and organisational security measures that are equivalent to those afforded to live Personal Data; and
- The Firm and any relevant Processor have in place and must comply with a strategy for the permanent deletion, anonymisation, pseudonymisation or secure encryption of the Personal Data, complies and can demonstrate compliance with such policy.

1.16. Personal Data breaches

1.16.1. Internal reporting

Whenever a personal data breach occurs, this must be reported to the Firm's [DPO], SEO and Compliance Officer.

A personal data breach is breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Upon receipt of the internal report, the Compliance Officer investigates the matter, formalizes his investigation in a report addressed to the SEO and determines whether there is a requirement to notify the DIFC Data Protection Commissioner and Data Subject.

The Compliance Officer maintains a register of reported personal data breaches and reports on this in his periodic reporting to the Board.

1.16.2. Notification of Personal Data Breaches to the Data Protection Commissioner

If there is personal data breach that compromises a Data Subject's confidentiality, security or privacy, the Firm notifies as soon as practicable in the circumstances, the personal data breach to the Data Protection Commissioner.

A Processor must notify the Firm without undue delay after becoming aware of a personal data breach

The notification to the Data Protection Commissioner:

- describes the nature of the personal data breach including where possible, the categories and approximate number of Data Subjects concerned, and the categories and approximate amount of personal data records concerned;
- communicates the name and contact details of the DPO or other contact point where more information can be obtained;
- describes the likely consequences of the personal data breach; and
- describes the measures taken or proposed to be taken by Firm to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

1.16.3. Notification of Personal Data Breaches to a Data Subject

When the personal data breach is likely to result in a high risk to the security or right of a Data Subject, the Firm must communicate the personal data breach to the affected Data Subject as soon as practicable in the circumstances.

This communication describes in clear and plain language the nature of the personal data breach and contains information on the likely consequences of the breach and the measures undertaken by the Firm to address the breach. The communicational also makes recommendations for the Data Subject to mitigate adverse effects.

Where a communication to the individual Data Subject will involve disproportionate effort, a public communication or similar measure whereby the Data Subjects are informed in an equally effective manner shall be enough.

1.17. Record keeping

The Firm must maintain a written record, which may be in electronic form, of processing activities under its responsibility, which contains at the least the following information:

- the Firm's name and contact details
- the name and contact details of the Data Protection Officer, where applicable;
- the purpose(s) of the Processing;
- a description of the categories of Data Subjects;
- a description of the categories of Personal Data;
- categories of recipients to whom the Personal Data has been or will be disclosed, including recipients in third countries and international organisations;
- where applicable, the identification of the third country or international organisation that the Personal Data has or will be transferred to;
- where possible, the time limits for erasure of the different categories of Personal Data; and
- where possible, a general description of the Firm's technical and organisational security measures.