Avenox Global Internal Data Protection Policy

AVENOX GLOBAL INTERNAL DATA PROTECTION POLICY

Effective Date: 4-13-26

Version: 1.0

1. Introduction

This Internal Data Protection Policy ("Policy") sets out the principles, standards, and procedures adopted by Avenox ("Avenox", "we", "us", "our") in relation to the collection, use, processing, storage, transfer, and protection of Personal Data in accordance with the DIFC Data Protection Law No. 5 of 2020 (as amended) ("DP Law").

Avenox shall ensure that Personal Data is processed lawfully, fairly, and transparently, and that appropriate technical and organisational measures are implemented to safeguard such data against unauthorized or unlawful processing, accidental loss, destruction, or damage, in accordance with applicable law.

This Policy applies to all employees, officers, contractors, consultants, and third parties acting on behalf of Avenox.

Personal data will be collected solely for lawful purposes, and all reasonably practicable measures will be taken to ensure the accuracy of any personal data held. We will also implement appropriate safeguards to protect such data against unauthorised or accidental access, processing, erasure, loss, or misuse. Where a data processor is engaged to handle personal data on our behalf, we will ensure—through contractual or other appropriate means—that such processor adheres to our data security standards. Personal data will only be used for the purposes for which it was originally collected, for purposes directly related to those original purposes, and as otherwise specified herein.

2. Definitions

- **Personal Data**: Any information relating to an identified or identifiable natural person.
- **Special Category Data**: Sensitive personal data including racial origin, political opinions, religious beliefs, health data, biometric data, and, in a compliance context, criminal, sanctions, and regulatory data.
- **Processing**: Any operation performed on Personal Data, including collection, storage, use, disclosure, or deletion.
- **Controller / Processor**: As defined under the DP Law.

3. Role of Avenox: Controller and Processor

Depending on the nature of the engagement, Avenox may act as:

- **Data Controller**, where Avenox determines the purposes and means of processing (e.g., internal operations, employee data);
- **Data Processor**, where Avenox processes Personal Data on behalf of clients under documented instructions;
- **Joint Controller**, where purposes are jointly determined.

Avenox will clearly identify its role in each engagement and comply with corresponding obligations under the DP Law.

4. Data Protection Principles and Implementation

4.1 Lawfulness, Fairness and Transparency

Processing shall be conducted on a lawful basis under Article 13 of the DP Law. Avenox shall ensure Data Subjects (clients, partners, employees) are informed of processing activities through clear and accessible notices.

4.2 Purpose Limitation

Your personal Data shall only be collected for specified, explicit, and legitimate purposes and shall not be further processed in a manner incompatible with those purposes.

4.3 Data Minimisation

Avenox shall implement internal controls to ensure only necessary data is collected, including restricted data access, role-based permissions, and controlled data intake processes.

4.4 Accuracy

Avenox shall implement procedures to maintain data accuracy, including periodic reviews, client confirmations, and updates where required. All data subjects shall review our website for new/updated data protection policies.

4.5 Storage Limitation

Data shall be retained only for defined periods 5–10 years depending on regulatory requirements.

4.6 Integrity and Confidentiality

Avenox shall implement technical and organisational measures including encryption, secure storage, and access controls.

4.7 Accountability

Avenox shall maintain records, policies, and procedures demonstrating compliance with the DP Law.

5. Types of personal data collected

5.1 Identification Data

Identification data includes, full name, nationality, passport or ID details, date of birth and any such information required for Identity verification and for Avenox to provide its service or complete its contractual obligations and to complete its due diligence for compliance with KYC obligations.

5.2 Contact Data

“Contact Information” refers to any information that enables us to communicate with you, including, but not limited to, your name, username, mailing address, telephone number(s), email address, or any other details through which messages may be delivered to you.

5.3 Professional and Relationship Data

“Relationship Information” refers to information that facilitates our business relationship with you, including, but not limited to, the types of products and services we provide to you or that may be of interest to you, as well as details regarding your job title, company’s size, geographic presence, creditworthiness, Business relationships and demographic profile. This information may also include your

5.4 Financial and Compliance Data

Includes:

- Source of funds and source of wealth
- Banking and transaction-related information
- AML/KYC documentation
- Politically Exposed Person (PEP) status
- Sanctions or adverse media information

Purpose and Importance: This data is critical for:

- Conducting Anti-Money Laundering (AML) checks
- Assessing financial risk and legitimacy of funds
- Ensuring compliance with UAE and international regulations
- Protecting clients and the firm from financial crime risks

Collecting this data ensures that:

- Business transactions are lawful and transparent

- Clients meet regulatory requirements
- Avenox can provide accurate compliance advisory

5.6 Communication Data

Communication data refers to Emails, meeting minutes, or any call records we deem worthy of recording. The purpose of keeping communication data is to maintain records of communication for service delivery, relationship management, and compliance documentation.

5.7 Employee Data

If you apply for a role or work with Avenox, we may collect:

- Employment history
- Professional qualifications and education
- Nationality and residency status
- References and background checks
- Identification documents

We may also review publicly available professional information (e.g., LinkedIn profiles) where relevant.

Purpose:

- To assess suitability for employment
- To comply with employment and immigration regulations
- To manage internal operations and HR processes

Avenox does not knowingly process Personal Data of minors.

6. Legal Basis for Processing your personal data (other than consent), how we use that personal data and whom we share it with (Article 13)

Processing shall be based on:

6.1. Contractual necessity;

We may process your personal data where such processing is necessary for the performance of a contract to which you are a party, or in order to take steps at your request prior to entering into such a contract. In this context, your personal data may be used for the following purposes:

- To prepare and provide you with proposals in relation to our services;
- To deliver services in accordance with our services agreement, terms of engagement, or as otherwise agreed with you from time to time;
- To address and manage any complaints, inquiries, or feedback you may submit;

- To fulfil any other purpose for which you provide personal data in connection with a contractual relationship; and
- To conduct background checks and pre-employment screenings, including in relation to job applicants and employees.

6.2. Legal obligation

We process personal data to fulfill our statutory and regulatory mandates. This includes, but is not limited to, the following activities:

- Regulatory Fulfillment: Adhering to established legal frameworks, such as anti-money laundering (AML) and "know your customer" (KYC) regulations.
- Judicial and Tax Mandates: Disclosing information as required by tax authorities, courts of competent jurisdiction, or other governing bodies.
- Oversight and Due Diligence: Recording communications (including telephone and email) and performing background or pre-employment screenings to satisfy regulatory standards.
- Crime Prevention: Detecting, preventing, and assisting in the investigation of illicit activities in cooperation with law enforcement and relevant authorities.

6.3. Legitimate interests

Avenox, as a compliance consulting firm, may process personal data when it is necessary for the purposes of its legitimate interests or those of its clients, provided such interests are not overridden by the fundamental rights and freedoms of the data subjects. Under the DIFC Data Protection Law No. 5 of 2020, these interests specifically include

- The provision of management consultancy services
- **Client Engagement and Development:** To provide marketing communications (subject to the "Marketing" section below), enhance our service offerings, and strengthen our professional relationship with you.
- **Legal Protections and Fraud Prevention:** To safeguard our rights, the rights of our clients, or your personal safety; and to detect, prevent, and mitigate fraudulent activity.
- **Legal Proceedings and Professional Advice:** To obtain legal counsel regarding our rights and obligations, and to manage the defense, prosecution, or initiation of legal claims involving you, the firm, or a third party.

By relying on this basis, Avenox ensures the operational continuity and integrity of its compliance advisory services while maintaining a high standard of data protection through necessary and proportionate processing measures.

Consent shall be taken where required.

7. Data Retention

- AML/KYC: 5–10 years;
- Client data: duration + retention period;
- Employee data: statutory period.

Data shall be securely deleted upon data subject's request, or after the completion of required data retention period or anonymized thereafter.

8. Data Sharing and Third Parties

We may share personal data with:

- Regulatory authorities if needed
- **Professional Consultants:** Our legal, financial, or other expert advisers, to the extent necessary to obtain professional guidance or specialized assistance.
- **Financial institutions**: Financial institutions include Banks, Audit and Assurance Providers: External auditors, where disclosure is required for the fulfillment of their statutory or contractual auditing mandates.
- **Verification Service Providers:** Authorized third-party agencies engaged to facilitate comprehensive background screenings and due diligence inquiries. Service providers (IT systems, CRM tools)
- Business partners and advisors where required.

All third parties are required to maintain confidentiality and data protection standards.

9. International Data Transfers (Article 27)

Personal data may be transferred outside the DIFC, mainland, UAE, where necessary for business operations or to provide client a service, in which case we would have already signed a service contract with them.

We ensure:

- Transfers are made to trusted jurisdictions
- Appropriate safeguards and contracts are in place
- To adequate jurisdictions; or
- Under appropriate safeguards; or
- With explicit consent.

Avenox shall conduct transfer risk assessments prior to such transfers.

10. Data Subject Rights and Requests

- **Access their personal data:** Data subjects have the right to confirm whether a controller is processing their data and, if so, to receive a copy of that data along with details about why and how it is being used.
- **Request correction (Rectification):** Individuals can require a controller to rectify inaccurate or incomplete personal data without undue delay to ensure their information is correct and up to date.
- **Request deletion (Erasure):** Also known as the "right to be forgotten," this allows individuals to request the permanent removal of their data when it is no longer necessary for its original purpose or if the processing is otherwise unlawful.
- **Object to processing:** Data subjects can object to the processing of their data in specific circumstances, such as for direct marketing purposes or when the processing is based on the "legitimate interests" of the firm.
- **Withdraw consent:** If an individual previously gave permission for their data to be processed, they have the absolute right to take back that consent at any time, requiring the firm to stop the related processing activity.
- **Lodge a complaint with the DIFC Commissioner:** If an individual believes their rights have been violated or that a firm is not complying with the law, they may formally report the matter to the DIFC Commissioner's office for investigation or mediation.

Please note that the above rights are not absolute, and we may be entitled to refuse requests where exceptions apply.

Requests shall be handled via:

Email: enquiry@avenoxglobal.com
Phone: +971 4 549 1026

Avenox shall respond within applicable timelines and maintain records of such requests.

11. Record of Processing Activities (Article 15)

Avenox maintains ROPA including processing purposes, categories, recipients, transfers, retention, and safeguards.

12. Data Security and Breach Management

We implement:

- Secure storage systems
- Access controls
- Monitoring and protection systems

In case of a data breach:

- The DIFC Commissioner will be notified (Article 41)
- Affected individuals will be informed where necessary (Article 42)

13. Marketing and Communications

Avenox may periodically issue marketing communications regarding our service offerings, industry alerts, newsletters, and invitations to professional events that we believe align with your interests. Such communications may be transmitted through various channels, including postal mail, telephonic contact, email, SMS, or other electronic platforms.

You maintain an absolute right to opt out of promotional communications at any time and at no cost. You may exercise this right through any of the following methods:

- **Electronic Opt-Out:** Utilizing the “unsubscribe” hyperlink or instructions provided within our marketing emails or mobile applications.
- **SMS Revocation:** Following the "Reply To" instructions contained within a marketing text message.
- **Direct Notification:** Informing our representatives of your preference to discontinue marketing during a telephone call.
- **Written Request:** Contacting us via the details provided in the “Queries and Contact Details” section to formally request the cessation of communications across any or all channels.

Service-Related Announcements Please note that Avenox may continue to distribute non-promotional, service-related announcements when necessary (e.g., critical updates regarding new legislation, regulatory changes, or compliance mandates). As these communications are essential for the fulfillment of our professional obligations and are not marketing in nature, they are generally not subject to opt-out requests.

14. Cookies and Tracking

Avenox may use cookies for analytics, security, and performance optimization.

15. Governance and Responsibility

Avenox has designated internal responsibility for data protection compliance and conducts periodic reviews of this Policy.

16. Contact Information

Email: enquiry@avenoxglobal.com
Phone: +971 4 549 1026

End of Document

Safe passage in a complex world