Data Protection and Privacy Policy

INGOT Financial Services L.L.C.

Revision Date:

1. Introduction:

Personal Data Protection Law

The Personal Data Protection Law, Federal Decree Law No. 45 of 2021 regarding the Protection of Personal Data, constitutes an integrated framework to ensure the confidentiality of information and protect the privacy of individuals in the UAE. It provides a proper governance for data management and protection and defines the rights and duties of all parties concerned.

Here are some of the provisions of the law in brief:

- The provisions of the law apply to the processing of personal data, whether in full or part through electronic systems, inside or outside the country.
- The law defines the controls for the processing of personal data and the general obligations of companies that have personal data to secure it and maintain its confidentiality and privacy. It prohibits the processing of personal data without the consent of its owner, except for some cases in which the processing is necessary to protect a public interest or to carry out any of the legal procedures and rights.
- The law gives the owner of the data the right to request for corrections of inaccurate personal data and to restrict or stop the processing of his personal data.

It sets out the requirements for the cross-border transfer and sharing of personal data for processing purposes.

Other laws related to data protection and privacy include:

Consumer protection law

The Federal Law No. 15 of 2020 on Consumer Protection protects all consumer rights, including the data of the consumers and prohibits suppliers from using it for marketing.

Protecting data and privacy online

Internet Access Management (IAM) policy

Telecommunications and Digital Government Regulatory Authority (TDRA) implements the Internet Access Management (IAM) policy in the UAE, in coordination with National Media Council and Etisalat and Du, the licensed internet service providers in the UAE. Under this policy, online content that is used for impersonation, fraud and phishing and/or invades privacy can be reported to Etisalat and Du to be taken down.

Electronic Transactions and Trust Services law

The law regulates the validity of electronic documents and boosts the legal value of digital signature and the level of its security. It provides provisions for eTransactions, the way eDocuments should be stored and saved, and sent and received to be valid. It also sets licensing requirements for trust services providers who are duly licensed to create, validate and preserve eSignatures, eSeals and digital certification.

The UAE's Constitution

Article 31 of the UAE's Constitution provides for the freedom of communication by means of post, telegraph or other means of communication and guarantees their confidentiality in accordance with the law.

Protection of copyrights, patents and trade marks

As a regulated company by SCA operating in UAE, INGOT Financial Services L.L.C. (the "Company") is committed to protecting the privacy, confidentiality and security of customer data. This data policy outlines the measures we take to ensure the protection of our customers' personal data in accordance with The Personal Data Protection Law and other relevant legislation.

2. Definitions

"Business purposes"- the purposes for which personal data may be used by us: personnel, administrative, financial, regulatory, payroll and business development purposes.

Business purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and good practice.
- Gathering information as part of investigations by regulatory bodies or in connections with legal proceedings or requests.
- Operational reasons such as recording transactions, training, and quality control ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking.
- Investigation complaints.
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct, disciplinary matters.
- Marketing our business
- Improving our services.

"Data Subject" A Natural Person who is the subject of Personal Data.

"Consent" The consent whereby the Data Subject authorizes a third party to process his/her Personal Data, provided that this consent 5 Federal Decree by Law Concerning the Protection of Personal Data indicates, in a specific, clear and unambiguous manner, that he/she accepts the processing of his/her Personal Data through a clear positive statement or action.

"Personal data"- Any data related to a specific natural person or related to a natural person that can be identified directly or indirectly by linking the data, through the use of identification elements such as his/her name, voice, image, identification number, his/her electronic identifier, his/her geographical location, or by one or more physical, physiological, economic, cultural or social characteristics. It includes Sensitive Personal Data and Biometric Data

"Processing"- Any operation or set of operations performed on Personal Data using any electronic means, including processing and other means. This processing includes collecting, storing, recording, organizing, adapting, modifying, circulating, altering, retrieving, exchanging, sharing, using, characterizing, disclosing Personal Data by broadcasting, transmitting, distributing, making available, coordinating, merging, restricting, blocking, erasing or destroying it or creating forms thereof.

"Sensitive Personal Data"- Any data which directly or indirectly reveals a natural person's family, ethnic origin, political or philosophical opinions, religious beliefs, criminal record, biometric data, or any data relating to such person's health and physical, psychological, mental, genetic or sexual condition, including information related to the provision of healthcare services to him/her which reveals his/her health status.

"Office"- This is the national body responsible for data protection. The supervisory authority for the Company is The UAE Data Bureau established under the aforementioned Federal Decree by Law No. (44) of 2021.

3. Scope of the policy

This policy applies to staff, who must be familiar with this policy and comply with its terms.

The policy outlines the procedures which the Company follows in order to protect personal data and ensures that the staff understands the rules governing the use of personal to which they have access during the course of their work. In particular this policy requires staff to ensure that the appointed Data Protection Officer (DPO) will be consulted before any significant new data processing activity is initiated, to ensure that relevant compliance steps are addressed.

The Company reserves its right to supplement or amend this policy by additional policies and guidelines from time to time, if necessary. Any new or modified policy will be circulated to staff before being adopted.

The appointed data protection officer (DPO) has overall responsibility for the day-to-day implementation of this policy.

4. The Personal Data Processing Controls :

Personal Data shall be processed according to the following controls specified in the law:

1. Processing shall be carried out in a fair, transparent and lawful manner.

2. Personal Data shall be collected for a specific and clear purpose. It shall not be processed at any later time in a manner incompatible with such purpose. However, it may be processed if the purpose is similar or close to the purpose for which this data is collected.

3. Personal Data shall be sufficient and limited to what is necessary in accordance with the purpose for which the processing is carried out.

4. Personal Data shall be accurate and correct and shall be updated whenever necessary.

5. The necessary measures shall be taken to ensure that incorrect Personal Data is deleted or corrected. 6. Personal Data shall be kept securely, including protecting it from any violation, penetration, or illegal or unauthorized processing through the development and use of appropriate technical and organizational measures and procedures in accordance with the laws and legislation in force in this regard.

7. Personal Data shall not be kept after the purpose of its processing has been exhausted. It may be kept if the identity of the Data Subject has been concealed using the "Anonymization Mechanism"

8. Any other controls set out in the Executive Regulations of this Decree by Law.

5. Collection and Processing of Personal Data:

We collect and process personal data only to the extent necessary for the provision of our services and compliance with legal requirements. Personal data is collected directly from the customer or from authorized third parties. Furthermore, the Company should always hold recent, clear, explicit and defined consent for the individual's data to be processed for a specific purpose.

Information the customer gives to the Company:

- identification data, such as name, surname, date of birth and nationality
- contact details, e.g. address, email address, mobile number
- identification documents (e.g. passport), photos, video and audio recordings and any other information provided for identification purposes to prove eligibility to use the Company's services
- details of bank account, debit or credit cards.
- data that chosen to provide us to obtain specific Services, such as delivery address or employment data in the course of application for our Business oriented services;
- information that given by communicating with us, whether by phone, email, online, or otherwise.
- data and content shared by you when participating in online discussions, surveys or promotions including those you post on our social media pages and community pages.
- photo (only if one is uploaded).
- Information we collect from you or generate about you
- personal details retrieved from your identification documents;
- information about the services you hold.
- information about the client's visit, including the links that have been clicked on, through and from the site (including date and time), services viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling and clicks), and methods used to browse away from the page, codes/tags that are used to identify human languages;
- technical information, including the internet protocol (IP) address used to connect to the internet, log-in information, the browser type and version, the time-zone setting, the operating system and platform, the type of device, a unique device identifier (for example,

the device's IMEI number, the MAC address of the device's wireless network interface), mobile network information, etc.;
- cookies and similar technologies we use to recognize the client, remember preferences and tailor the content we provide;
- risk rating information, e.g. transactional behavior and underwriting information;
- investigations and public information data, e.g. due diligence checks, sanctions and anti-money laundering checks;
- information that we need to support our regulatory obligations, e.g. information about transaction details, detection of any suspicious and unusual activity.

We process personal data for the following purposes:

1. Identity verification and anti-money laundering checks
2. Provision and management of financial services
3. Fraud prevention and detection
4. Compliance with legal and regulatory requirements

We do not use personal data for any other purpose than those stated above unless we have obtained explicit consent from the customer.

6. Sharing of Personal Data:

We may share personal data with the following third parties:

1. Financial service providers
2. Anti-fraud agencies
3. Regulators and supervisory authorities

We may also share personal data with other third parties with the explicit consent of the customer or as required by law. Also disclosures can be made in following cases:

- If disclosure thereof is reasonably necessary to perform particular financial service for the client.
- If the information is no longer confidential.
- If the disclosure is made upon request of judicial or supervisory entities in the state such as the SCA.

7. Security Measures:

We have implemented appropriate technical and organizational measures to ensure the security of personal data. This includes:

1. Access controls to personal data
2. Data encryption during transmission
3. Secure storage of personal data
4. Regular security audits and risk assessment

In cases, when data is stored on printed paper, it should be kept in a secure place, where unauthorized personnel cannot access it. Printed data should be shredded, when it is no longer needed. Data stored on a computer, should be protected by strong passwords, which are changed regularly. All staff use a password manager to create and store their passwords. Data stored on CDs or memory sticks, must be encrypted or password protected and locked away securely, when they are not being used. The DPO must approve any cloud used to store data. The server containing personal data is kept in a secure location and it is protected by security software. Data is regularly backed up in line with the Company's backup procedures, and it should never be saved directly to mobile devices such as laptops, tablets, or smartphones. All possible technical measures must be put in place to keep data secure.

8. Retention of Personal Data:

We retain personal data only for as long as necessary to fulfill our legal and regulatory obligations or for the purposes for which it was collected. Once the data is no longer required, we will securely delete or anonymize it. The period of retention depends on the for but stances of each case, considering the reasons which the personal data was obtained for, but should be determined in a manner consistent with the data retention guidelines. Under Applicable Regulations, the Company shall keep records containing Client personal data, trading information, account opening documents, communications, and anything else, which relates to the Client for at least five years, after the termination of the Business Relationship with the Client.

9. Rights of Data Subjects:

Customers have the right to:

1. Access their personal data
2. Correct any inaccuracies in their personal data
3. Request the deletion of their personal data
4. Object to the processing of their personal data
5. Request the restriction of the processing of their personal data
6. Receive a copy of their personal data in a structured, commonly used and machine-readable format

We will respond to all requests within one month and will provide the information free of charge unless the request is manifestly unfounded or excessive.

10. Third parties

The Company must have written contracts in place with any third-party data controllers and/or data processors which it is planning to enter into an agreement with. The agreement must contain specific clauses, which set out the Company`s and third-party liabilities, obligations, and responsibilities. The Company must only appoint processors who can provide sufficient guarantees under the law and that the rights of data subjects will be respected and protected.

11. Data Protection Officer:

11.1 Responsibilities of the Data Protection Officer (DPO)

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees, who wish to know, which data is being held on them by the Company
- Verifying the quality and correctness of the procedures in place at the company.
- Receiving requests and complaints related to Personal Data in accordance with provisions of this Decree-Law and its Executive Regulations

- Providing technical advice on evaluation procedures and periodic examination of personal data protection systems and intrusion prevention systems at the company, documenting the results of such evaluation and providing appropriate recommendations in this regard, including risk assessment procedures.
- Any other tasks or powers which are determined in accordance with the Executive Regulations of this Decree by Law.

The Data Protection Officer shall maintain the confidentiality of information and data it receives in implementation of its duties and powers in accordance with provisions of this Decree by Law and its Executive Regulations and in accordance with the legislations in force in the State.

We have appointed a Data Protection Officer (DPO) who is responsible for overseeing our data protection practices. The DPO can be contacted at info@ingot.ae

When assessing appropriate technical measures, the Data Protection Officer/GDPR Owner will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the company's premises such as laptops;
- Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- Regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation; and
- Identifying appropriate international security standards relevant to INGOT Financial Services L.L.C.

When assessing appropriate organizational measures, the Data Protection Officer will consider the following:

- The appropriate training levels throughout INGOT Financial Services L.L.C.
- Measures that consider the reliability of employees (such as references etc.);

- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper-based records;
- Adoption of a clear desk policy;
- Storing of paper-based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employees own personal devices being used in the workplace;
- Adoption of clear rules about passwords;
- Making regular backups of personal data and storing the media off-site; and
- Taking appropriate security measures when transferring data outside UAE and the imposition of contractual obligations on the importing organizations.

These controls have been selected, based on identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

12. Training

Adequate training on provisions of data protection regulation will be provided to all employees, customized according to their position. If any employee changes his/her position and/or responsibilities and he/she is responsible for requesting new data protection training, relevant to that new role or/and responsibilities will be provided.

13. Data Protection Risks

This policy helps to protect INGOT Financial Services L.L.C. from potentially, serious data security risks, including:

- Breaches of confidentiality: for instance, information processed inappropriately;
- Reputational damage: for instance, the Company could suffer material or non-material damage if hackers successfully gained access to sensitive data.

14. Regular review

Assessments of the Company's Data protection policies will be completed in the annual review process or monthly Governance and Risk Committee to ensure the company remains compliant.

This Policy will also be reviewed annually or as required. Any review will be approved by the Governance, Risk and Compliance Committee in the first instance. All relevant stakeholders and decision makers will be consulted prior to final approval from the Board.

Conclusion:

We are committed to protecting our customers' personal data and will continue to review and improve our data protection measures in line with the latest legal and regulatory requirements.