Data Protection Policy of
ITSAGA FINANCIAL LTD

Contents

Tables

Introduction

Welcome to ITSAGA Financial Ltd's Privacy Policy.

ITSAGA Financial Ltd (referred as "ITSAGA", the "Organization"), respects your privacy and is committed to protecting your personal data. This privacy policy explains how we look after your personal data when you visit our website, become a client or visit our premises. It also informs you of your privacy rights and how the law protects you.

This policy outlines how we collect, process, store, and protect personal data in compliance with the General Data Protection Regulation (GDPR) 2016/679 and relevant Cyprus data protection laws "The Protection of Physical Persons Against the Processing of Personal Data and Free Movement of such Data Law 125(I)/2018".

This policy applies to all systems, people, and processes that constitute the organization's information systems, including board members, directors, employees, suppliers, and other third parties with access to ITSAGA's systems.

Privacy and personal data protection policy

The General Data Protection Regulation

The General Data Protection Regulation 2016 (GDPR) is one of the most significant pieces of legislation affecting the way that ITSAGA carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of citizens of the European Union. It is ITSAGA's policy to ensure that our compliance with the GDPR and other relevant legislation is always clear and demonstrable.

Definitions

Personal data is defined as: *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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 the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

Processing means: *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."*

Controller means: "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."*

Principles relating to processing of personal data

There are several fundamental principles upon which the GDPR is based.

These dictate that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation').
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
4. Accurate and, where necessary, kept up to date ('accuracy')
5. 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 ('storage limitation').
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

In addition, the controller shall be responsible for and be able to demonstrate compliance with all these principles ('accountability').

ITSAGA ensures that it complies with all these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems.

Data Collected and means of collection

Information can be obtained in various ways, including but not limited to:

a) Client Registration through Website: When a prospective client registers interest through our website (e.g., wire wallet platform), their data is submitted via API to our internal CRM.
b) Client Evaluation by Partners: The client data may be shared with selected partners via email or partner portals to evaluate whether the client meets onboarding criteria.
c) Client Onboarding via Partner CRM: Upon approval, clients are onboarded directly through our partners' CRM systems. We maintain ongoing coordination throughout this process.
d) Information that we collect through regulatory authorities or financial institutions as part of compliance and due diligence processes.

ITSAGA collects, uses, stores, processes, and transfers different kinds of personal data, such as:

- **Identity Data:** Includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth, gender, and ID (only for onboarding and compliance procedures).
- **Contact Data:** Includes name, surname, billing address, email address, and telephone numbers.
- **Sensitive Data:** Includes health-related information only where required by employment regulations or accessibility accommodations.
- **Financial Data:** Includes bank account and payment card details, salary details, tax identification number (TIN), VAT number (for companies), financial statements, payroll information, social insurance records, other tax-related documents, and monthly transaction totals received from banking institutions.
- **Transaction Data:** Includes details about payments to and from clients, invoices, records of professional services rendered, and corporate bank agreements.
- **Marketing and Communications Data:** Includes your preferences in receiving marketing materials from us and our third parties, and your communication preferences.

- **CCTV Data:** Includes images from areas external and internal to the accounting office, such as entrances/exits, corridors, client meeting areas, and financial document storage zones.
- **Technical Data (employees only):** Includes internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices used to access our online services.
- **Usage Data:** Includes information about how you use our website, collected via cookies and other tracking technologies.

Lawful basis of processing

When processing personal data ITSAGA ensure that it is based in at least one of the following Lawful basis:

- Legitimate interest: Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
- Contractual obligation: Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Legal obligation: Processing is necessary for compliance with a legal obligation to which the controller is subject
- Consent: The data subject has given consent to the processing of his or her personal data for one or more specific purposes

Use of Data

ITSAGA collects and processes your data for the following purposes:

- To assess whether our services are suitable for prospective clients.
- To evaluate the eligibility of a client for onboarding and determine service compatibility.
- To share client data with partners for evaluation and onboarding decisions.
- To onboard clients via partner CRM systems and coordinate the associated administrative steps.
- To notify clients regarding the outcome of their application (accepted, rejected, or in process).
- To validate client activity through monthly transaction data received from banking providers.
- To assess and archive corporate bank agreements received during onboarding.
- To meet employment-related obligations including payroll processing, labor law compliance, and employee management.
- To comply with applicable legal, regulatory, tax, or anti-money laundering (AML) requirements.
- To ensure the confidentiality and security of personal and financial data, including fraud prevention and cyber protection.
- To enhance service quality through analytics, business intelligence, and operational

performance review.

- To improve internal operations and facilitate effective management of client services.
- To manage communication and marketing preferences and send updates or regulatory insights where appropriate.
- To ensure the safety and security of employees and visitors through CCTV monitoring and controlled access.

Joint Controller Arrangements

In the context of client onboarding, ITSAGA may act as a joint controller together with its onboarding partners. This arrangement is established to jointly determine the purposes and means of processing personal data for onboarding purposes. Responsibilities under Article 26 GDPR are defined in contractual agreements between the parties.

Direct Marketing

PROMOTIONAL OFFERS FROM US

We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you (we call this marketing).

You will receive marketing communications from us if you have requested information from us or purchased services from us and you have not opted out of receiving that marketing.

Prior consent is required for electronic direct marketing, i.e. newsletters, emails containing promotion, advertisements, texts or automated calls. There is, however, a limited exception for existing customers known as “soft opt in”, which allows organisations to send marketing texts or emails if they have already obtained contact details in the course of a sale to that person or they are marketing similar products or services or they have already given the person an opportunity to opt-out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing is explicitly provided to the data subjects in an intelligible manner, so that it is clearly distinguishable from other information.

THIRD-PARTY MARKETING

We will get your express opt-in consent before we share your personal data with any third party for marketing purposes.

You can ask us or third parties to stop sending you marketing messages at any time by logging into the website and checking or unchecking relevant boxes to adjust your marketing preferences or by following the opt-out links on any marketing message sent to you or] by *Contacting us* at any time.

OPTING OUT

The objection of the data subjects to direct marketing is promptly honoured. In case a data subject opts out at any time, their details are suppressed as soon as possible, and processing is forbidden. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Where you opt out of receiving these marketing messages, this will not apply to personal data

provided to us as a result of [a product/service purchase, warranty registration, product/service experience or other transactions].

Methods of Processing

- **Manual Processing:** Personal data may also be processed manually by our trained staff, who handle data securely and confidentially.
- **Data Transfers:** Personal data may be transferred to third-party service providers who assist us in our operations. These providers comply with data protection laws and maintain a high level of data security.

Sharing with Third Parties

ITSAGA shares personal data with trusted partners only for onboarding and service delivery purposes. These parties include:

- Onboarding partners who assess and process client applications.
- Cloud-based CRM providers.
- Financial institutions providing transaction reports or processing bank agreements.

All such sharing is subject to:

- Data Processing Agreements (DPAs) in line with Article 28 GDPR
- Joint Controller Agreements (JCAs) where applicable
- Role-based access controls and appropriate technical safeguards

Transfer of personal data outside of the European Economic Community

ITSAGA does not normally transfer Personal Data outside of the European Economic Community.

Where none of the appropriate safeguards are applicable, we may carry out the transfer on the basis of at least one of the specific situations, i.e. the data subject's specific consent, necessity for the performance of a contractual obligation etc. In addition, we will always take into account the relevant provisions under Cyprus Data Protection Law. In any event, we always make sure we take all reasonable and practicable measures to ensure the secure transfer in accordance with the GDPR.

Data retention

ITSAGA retains Personal Data as follows:

Data Category	Employees and Partners	Clients
Identity Data	7 years after termination	7 years after termination
Contact Data	7 years after termination	7 years after termination

Sensitive Data	7 years after termination	7 years after termination
Financial Data	12 years after termination	12 years after termination
Transaction Data	12 years after termination	12 years after termination
Technical Data (log files)	1 year	Not Applicable
Usage Data	6 months	6 months
Marketing and Communications Data	Until data subject opts-out	Until data subject opts-out
CCTV	Overwritten automatically	1 month

Personal Data of clients and employees are retained as long as they are actively interacting and then archived and retained according to Laws, Regulations and internal policies. ITSAGA implements all technical and organisational measures to safeguard the data for the full life cycle.

Data Deletion

ITSAGA deletes personal data when a) a reasonable data subject request occurs or b) the personal data are no longer required for operational, legislative or other, justifiable reasons. Consideration is also given as to whether information may be useful to the organization in anonymized form.

Methods of information deletion may vary according to the way in which the information is stored and may include:

- Automated deletion after a specified period of time (for example for email)
- Using secure deletion software to ensure that information may not be retrieved
- For information held on paper, shredding using a cross-cut shredder
- Physical destruction of storage devices such as hard drives
- Manual deletion of information once no longer required (for example, temporary files at the end of a project)
- Restoration of factory settings (for example in the case of a mobile device)

Rights of the individual

The data subject also has rights under the GDPR. These consist of:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing

- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Each of these rights is supported by appropriate procedures within ITSAGA that allow the required action to be taken within the timescales stated in the GDPR. These timescales are shown in Table 1.

DATA SUBJECT REQUEST	TIMESCALE
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	Within One month
The right to rectification	Within One month
The right to erasure	Within One month
The right to restrict processing	Within One month
The right to data portability	Within One month
The right to object	Within One month
Rights in relation to automated decision making and profiling.	Within One month

Table 1: Timescales for data subject requests

Other rights include: the right to be notified of a Personal Data Breach which is likely to result in high risk to your rights and freedoms; the right to make a complaint to the Supervisory Authority; the right to withdraw consent to Processing at any time.

Please note that these rights are not absolute and subject to exceptions. These therefore may be limited where ITSAGA has an overriding interest or legal obligation to continue to process the data or where data may be exempt from disclosure under applicable law. The applicability of data subjects' rights depends on the legal basis on which ITSAGA relies in each case.

The data subjects can request the exercise of their rights by sending e-mail to dpo@wire-wallet.com.

If data subjects wish to raise a complaint on how ITSAGA handled their Personal Data, they may contact the Company to have the matter investigated.

If they are not satisfied with ITSAGA's response, they may lodge a complaint to:

Office of The Commissioner for Personal Data Protection

Office address: Iasonos 1, 1082 Nicosia, Cyprus

Postal address: P.O.Box 23378, 1682 Nicosia, Cyprus

Tel: +357 22818456

Fax: +357 22304565

Email: commissioner@dataprotection.gov.cy

Privacy by design

ITSAGA takes all appropriate security measures to ensure that the personal data/data collected and stored in connection with your visit to the website and/or in relation to the services and products provided by ITSAGA is protected against any unauthorized access, misuse, loss and/or destruction.

ITSAGA uses physical and electronic security measures, including but not limited to the use of firewalls, personal passwords, encryption and authentication technologies. ITSAGA's employees and service providers are bound by professional secrecy and must comply with all data protection provisions.

It is to be noted, that access to personal data is restricted to specific employees, contractors and third-party service providers who require this access in order to process the agreement between ITSAGA and you, all on a "need to know" basis and to be able to execute all obligations emanating from the agreements in place. Use of techniques such as data minimization and pseudonymisation will be considered where applicable and appropriate.

Data protection officer

ITSAGA has appointed a Data Protection Officer (DPO, who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the DPO using the details set out below.

Contact details for the Data Protection Officer are as follows:

Email: dpo@wire-wallet.com

Tel: +357 24 828 623

Address:

22, Archbishop Makarios III, MAKARIA CENTER, 5th floor, office 501, Larnaca, Cyprus

Corporate website: www.wire-wallet.com.

Self-Assessment of Legal Compliance

ITSAGA conducts a self-assessment regarding personal data and its compliance with relevant legal provisions. This self-assessment is carried out using appropriate methodologies developed by the organization or from a reliable external source. The self-assessment is repeated annually, with results retained and necessary compliance measures implemented.

Third-Party Links

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

Cookies

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly. For more information about the cookies we use, please see our Cookies Policy.

Review and Update of Data Protection Policy

ITSAGA reviews and updates its Data Protection at least annually or when a significant change to the processing activities occurs.

Last Update 04 March 2025.

ITSAGA Financial Ltd,

22, Archbishop Makarios III, MAKARIA CENTER, 5th floor, office 501, Larnaca, Cyprus

+357 24 828 623