PERSONAL DATA PROTECTION POLICY

Date Created: 1 January 2019
Last Updated: 1 August 2019

General

This Personal Data Protection Policy sets out how ISM Group of companies (the "**Organization**") processes data of its employees, clients, business associates and other interested parties. This Policy has been prepared in accordance with the provisions of the EU General Data Protection Regulation ("**GDPR**").

Any questions relating to this Policy or requests in respect of personal data should be directed to our internal legal advisor, Mr. Antonis Vryonidis, at the following email: dataprotection@iswm.eu.

Who we are

The Organization consists of various companies with a diversified portfolio of high-performing quality assets and trading activities in various countries of the world.

The Organization strives to protect personal data and apply high standards of conduct when it comes to privacy issues. It ensures that its employees are provided with the appropriate training in order to handle personal data promptly and in accordance with the laws. Furthermore, the Organization endeavors to ensure that any parties with whom it co-operates apply the same high standards when it comes to data protection and privacy.

Summary

This Policy is applicable to processing of your personal data by the Organization and explains:

1. what personal data we process about you;
2. why (for what purposes) we process your personal data (including the legal grounds for your data processing);
3. how and where we process your personal data;
4. what are your rights;
5. security of processing;
6. retention of data; and
7. use of personal data in legal proceedings.

Changes to this Policy

The Organization keeps this Policy under review in order to ensure that it is in line with any changes to the laws relating to privacy and personal data protection. This Policy was last updated on 1 August 2019.

1. What data do we process?

The Organization processes data in the context of conducting its business. We process the personal data that you provide to us, that we obtain from your employer or contractual partner, advisor or third party or that you explicitly made publicly available. The categories of data that may be collected and processed, according to the particulars of each case, include:

- personal details (including names, surnames, gender, occupation, postal addresses, email addresses and telephone numbers);
- information required by the Organization to meet legal and regulatory requirements or communicate with competent authorities (e.g. to comply with the anti-money laundering legislations, with taxation requirements etc.);
- information provided in the context of conducting its business, such as in entering into various agreements (e.g. employment agreement with its employees or other agreements with third parties);
- financial information, such as payment related information;
- any other information that may be provided to the Organization.

Important notice on Special Category Data

In certain instances, the personal data that the Organization processes may include "Special Category Data" (which includes information on a person's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data processed for the purpose of uniquely identifying a natural person, health data, data on a person's sex life or sexual orientation or data relating to a person's criminal record or alleged criminal activity). In such instances, legal bases for processing that data may include explicit consent (where the Special Category Data has been provided to the Organization by the data subject for any of the below-listed purposes) or the processing is being necessary for compliance with a legal obligation or for the purposes of bringing, pursuing or defending a legal claim. The Organization ensures that the retention of Special Category Data is in accordance with this Policy and that such data are properly destructed as soon as they are not necessary.

2. Why do we need them?

The Organization ensures that the data collected and processed is relevant to its processing activities and that the Organization does not collect or process more or less data than what is reasonably required for achieving the purpose of each processing activity. Furthermore, for each purpose of processing, there is always at least one lawful basis (under Article 6 of the GDPR – "Lawfulness of Processing") to secure that the rights of individuals are safeguarded by all means. Purposes for which the Organization may process personal data include:

- entering into agreements with its employees or third parties;
- identity verification and internal compliance;
- to ensure the security of the Organization's system, employees and premises;
- to meet all legal and regulatory obligations applicable to the Organization;
- to follow up on comments, enquiries and complaints;
- general contract administration and financial accounting (invoicing);

- any other purposes applicable to the Organization's business needs.

3. Sources and Recipients of data

The sources of data may include clients, intermediaries, data subjects directly, third parties connected to the data subject (for example, their employer or another service provider who provides services to the data subject) or open-source material.

Reasonable endeavors are made to ensure that data is only accessible by those with a need for access to fulfil the purposes set out above. Requests for access to be restricted in any particular manner should be made to the email mentioned above and will be considered and, where possible with reference to legal and regulatory obligations, actioned.

The following is a list of potential recipients of data (in each case including respective employees, directors and officers):

- employees of the Organization who are acquainted with the GDPR and who have a duty of confidentiality with regard to information obtained in the course of the employment with the Organization;
- service providers (legal, governmental or otherwise, including any bank or financial institution providing services in relation to any matter on which the Organization is instructed) where disclosure to that service provider is considered necessary to fulfil the purposes set out above;
- any sub-contractors, agents or service providers of the Organization;
- courts or tribunals in Cyprus or abroad;
- third parties with whom the Organization engages for conducting its business;
- law enforcement agencies where considered necessary for the Organization to fulfil legal obligations applicable to it;
- regulators or other governmental or supervisory bodies with a legal right to the material or a legitimate interest in any material;
- any registrar of a public register where the data is to be included in a public registry.

Unless expressly declared in this Policy or with the prior consent of the individual, personal data collected from an individual will not be disclosed to any third party other than the above-named parties. Each of the recipient(s) shall be responsible for ensuring the appropriate protection of your data, providing information on your data processing and obtaining additional consents when required.

Where the Organization is entering into an engagement with a third party pursuant to which data may be processed by that third party, the Organization will seek to enter into an agreement with that third party setting out the respective obligations of each party and it will seek to be reasonably satisfied that the third party has measures in place equal to those of the Organization to protect data against unauthorized or accidental use, access, disclosure, damage, loss or destruction.

In the event that any such third party is outside of the European Union and where the data being transferred would include personal data which would be protected under applicable Data Protection regulation the Organization will ensure that it meets the relevant requirements of that Data Protection

regulation prior to carrying out any such transfer. This may include only transferring the data where the Organization is satisfied that:

- the non-European Union country has Data Protection laws similar to the laws in the European Union;
- the recipient has agreed through contract to protect the information in the same Data Protection standards as the European Union;
- the relevant data subjects have consented to the transfer;
- if transferred to the United States of America, the transfer will be to organizations that are part of the Privacy Shield.

4. Rights of Data subjects

Data subjects in the European Union (or any jurisdiction with equivalent legislation to the GDPR) have certain rights in respect of their personal data. Any such data subject wishing to exercise any rights under applicable data protection laws (including the right to withdraw any consent to processing previously given; the right of access to data; or to have data corrected, updated, rectified or erased; or for access to data to be restricted or provided to any third party; or to object to any particular processing; or to lodge a complaint with the relevant supervisory authority; or the right to data portability) should send the request in the first instance to our internal legal advisor, Mr. Antonis Vryonidis, at the following email: dataprotection@iswm.eu.

In response to such requests, the Organization reserves the right to require the individual making the request to provide certain details about himself/herself so that the Organization can validate that the individual is indeed the person whom the data refers to. The Organization is required to respond to the request of the individual within 40 days and it will endeavor to do so wherever possible. The Organization reserves the right to charge a reasonable fee to cover any expenses that may arise from the request.

5. Security of processing

The Organization has established technological, physical, administrative and procedural safeguards all in line with the industry accepted standards in order to protect and ensure the confidentiality, integrity or accessibility of all personal data processed; prevent the unauthorized use of or unauthorized access to the personal data or prevent a personal data breach (security incident) in accordance with the Organization's policies and Data Protection Legislation.

6. Retention of data

The Organization retains personal data (including Special Category Data) in accordance with this Policy to fulfil the purposes for which the data was collected. After the fulfilment of the purposes for which the personal data was collected or within 5 years after the business relationship terminates, such data will be destroyed, unless destruction is prohibited for legal, regulatory or technical reasons. In the case of Special Category Data, the retention period after the termination of the business relationship shall be 1 year, unless retention for a longer period of time is required by or is justified under applicable law.

7. Use of Personal Data in Legal Proceedings

If it becomes necessary that the Organization has to take action against a third party for any reason whatsoever, including but not limited to recovering from any money owed to the Organization, the Organization shall have the right to rely on the personal data provided in identifying and taking legal action against that third party.