Privacy Notice for ISS Employees

Article 13, Data Protection Regulation 2016/679 – GDPR
Article 5, Personal Data Protection Law 45/2021 – PDPL

Effective Date: 24/01/2024

Version n.: 1.0

Data Controller

Pursuant to Article 13 of the EU Regulation 2016/679 (***GDPR***) and Article 5 of the UAE Federal Decree-Law No. 45 of 2021 (***PDPL***), **ISS Global Forwarding One Person Company LLC** (hereinafter "**ISS**", or "**Company**", or "**Data Controller**"), processes personal data from data subjects and their family's members during the recruitment process and during the employment relationship and provides this Privacy Notice to inform every subject with an active employment relationship with ISS about the nature of personal data processing activities pertaining to them.

Purposes and legal basis

Personal data are used for the sole purpose of the execution and management of the existing employment relationship. In detail, for the following purposes:

1. establishment and termination of the employment relationship and fulfillment of related obligations;
2. provision of salary, contributions, insurance and tax obligations;
3. planning and management of working activities (planning of tasks, work performance, access badges, etc.);
4. booking of services and tickets for travelling and transfers in execution of the employment relationship;
5. fulfillment of specific obligations or performing specific tasks arising from laws (e.g.: tax obligations, health and safety regulations, etc.), regulations or collective agreements, including company agreements;
6. fulfillment obligations to social security and welfare institutions, both mandatory and optional;
7. defense in legal proceedings;
8. fulfillment of obligations arising from insurance contracts aimed at covering risks related to the employer's liability for occupational health and safety;
9. business economic planning, arrangement of budgets and their management in the context of the execution of the employment contract;
10. performance of training and/or organizational activities;
11. control of the correct use of corporate assets (phones, PCs, tablets, etc.) for the verification of the correct and proper use of IT and system resources;
12. Internal access control activities (control of the security and integrity of corporate assets).

Personal data are necessary for the performance of pre-contractual and contractual measures taken in order to establish an employment relationship with data subjects (Art. 6 par. 1, let. b, GDPR and art. 4, PDPL) and for compliance with a legal obligation to which the Data Controller is subject (Art. 6 par. 1, let. c, GDPR, art. 4, par. 9, PDPL and art. 13 of Federal Decree-Law 33/2021).

Pursuant to point 12 of the abovementioned purposes, the internal access control measures will be implemented through:

- RFID technology badges for staff members;
- Fingerprint detection for warehouse specialized personnel;

The legal basis for this last processing of personal data will be the given consent of data subject (art. 6, par. 1 let. a, GDPR, art. 9, par. 2 let. a, GDPR and art. 4, PDPL), which will be required through a specific form attached below in the privacy notice, only to grant access to warehouses.

Personal data

The personal data processed for the aforementioned purposes are:

a) Common personal data (name, surname, address, date and place of birth, social security number, ID), contact information (phone number, email address), identification of the employee's family members, previous employment data, social security data, educational and work record, bank account details;

b) System data and company access information (ISS's emails, cloud-based systems, information systems, hardware and business facilities).

Special categories of personal data

Other personal data falling into the category of special data (Art. 9 GDPR and art. 1, PDPL), i.e., those capable of revealing **state of health**, **membership in a trade union**, **membership in a political party**, **racial and ethnic origin** or **religious beliefs** will be processed exclusively by personnel due to their tasks or hierarchical position within the organizational unit responsible for human resources management who will act under a confidentiality constraint, taking appropriate security measures and when required and permitted by the applicable law. In relation to the activity mentioned in point 12, fingerprint detection systems are implemented only for controlling warehouses access.

Data retention period

Personal data will be processed and stored for the duration of the employment contract and for the fulfillment of the related obligations, in any case in accordance with the terms applicable by relevant laws and regulations, as well as those prescriptions provided for the exercise of the rights deriving from the employment relationship even after its final termination. In any case, employees' data will not be kept more than 10 years from the date of termination of the employment relationship. In relation to the activity mentioned in point 12, it is established a data retention period of 2 years from the date of personal data collection.

Means of the processing

Data processing is performed through electronic means or paper media by persons specially appointed for the purposes highlighted above and committed to confidentiality. The data are protected by security measures aimed at preventing unauthorized access, loss or destruction.

Data communication

For the purposes instrumental to the execution of the current employment relationship, the Company can eventually transmit some of employees' personal data, according to a strict criterion of relevance, to the following categories of recipients:

- **institutions of patronage and social assistance**, employment agencies;
- **insurers** for the purpose of utilization of specific benefits to which the employee wishes to have access (health coverage, insurance reimbursements, etc.);
- **banks or other credit institutions** indicated by the employees for the payment of their fees;
- **Welfare and assistance funds** and **social security and welfare institutions** for the purpose of payment of economic benefits for sickness, maternity, temporary disability caused by accident and family allowance;
- **Pension funds**;
- **External consultants** for personnel recruitment, selection and evaluation, litigation management and legal assistance,

due to the mentioned relationships;

- Authorized **medical centers** for employment medical examinations;
- Authorized **tax assistance centers** for tax reporting;
- **Service companies** entrusted with specific management related to contractual obligations (payroll, meal tickets, etc.);
- **Companies in the ISS group** for administrative-accounting purposes;
- **Public security and judicial authorities**, when requested.

These entities will act as "Autonomous Data Controller" of their respective processing operations.

In some cases, the processing is performed by external organizations that realize services of various kinds on behalf of ISS (such as, by way of example, payroll management, personnel training, etc.), in their capacity as Data Processors as provided for in Article 28 GDPR and Articles 7,8, PDPL. Besides what has been previously stated, the employees' personal data will not be communicated or disseminated to unspecified third parties.

Nature of data provision

The processing of such information is entirely instrumental to the above-mentioned purposes and its provision is part of a series of contractual obligations. The provision of personal data is mandatory for the performance of the activities envisaged in the preceding paragraphs and any refusal to provide it will result in the impossibility of executing and managing the business relationship.

Data transfer

Employees' personal data could be transmitted abroad, in particular towards Europe, where other ISS' Group Societies have their legal offices. In the event of transfer of personal data abroad, the Company undertakes to assess the implementation of appropriate measures to ensure that the data is adequately protected at the destination, verifying that the entities importing the data are subject to an adequacy decision adopted by the European Commission, or by signing with them standard contractual clauses, approved by the European Commission, possibly supplemented by additional security measures where necessary. In the case of transfers to companies in the ISS group, the Company will ensure that these latter have adopted security measures in line with European standards, as mechanisms assessing the risk arising from the data transfer, aimed at identifying appropriate measures to support the transfer itself.

Exercise of data subject's rights

Any employee may, at any time, exercise the rights set forth below.

1. **Access to personal data**: to obtain confirmation that data are being processed and, if so, access to the following information: the purposes, the categories of data, the recipients, the retention period, the right to lodge a complaint with a Supervisory Authority, the right to request rectification or erasure or restriction of processing or opposition to the processing itself as well as the existence of an automated decision-making process;

2. **Request for rectification or erasure ("*right to be forgotten*")**: a data subject can request that the records containing his/her personal data, that ISS holds about him/her, are rectified if incorrect or deleted without undue delay in predetermined circumstances provided for in art. 17 GDPR and 15 PDPL;

3. **Restriction of Processing**: data subjects' rights to obtain from the Data Controller a restriction to the use of personal data concerning them under specific circumstances detailed in art. 18 GDPR and 16 PDPL;

4. **Objection to processing**: to object on grounds related to employees' data processing based on legitimate interest of ISS or automated decision making or profiling;

5. **Data Portability**: in the case of automated processing realized on the basis of consent or performing a contract, to receive in a structured, commonly used and machine-readable format the data concerning the employee;

6. **Withdrawal of consent**: to the processing for the above-mentioned purposes; the exercise of this right does not affect in any way the lawfulness of the processing carried out before the withdrawal;

7. **Lodge a complaint**: under Article 77 GDPR and 24 PDPL with the Competent Supervisory Authority; for Italy, the

competent authority is the *Garante Per La Protezione Dei Dati Personali*, which can be contacted through the contact details provided in the following website *http://www.garanteprivacy.it*.

Requests relating to the exercise of the data subjects' rights will be processed within one month from the initial request; in cases of particular complexity and relevant number of requests this term may be extended by further 2 (two) months.

Points of contact for data subjects

Data subjects, for matters concerning the processing of personal data, can contact the Company at the following email address: **privacy@iss-gf.com** or ISS' Group Privacy Officer at the following email address: **GPO@iss-gf.com**.

Changes and updates

This Privacy Notice is effective from the date indicated in its header. The Company may also make changes and/or additions to this Notice, including as a consequence of any subsequent changes in the relevant applicable regulations.

Consent to the processing of personal data in accordance with Regulation (EU) 2016/679 on the protection of personal data (GDPR) and Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (United Arab Emirates) (PDPL)

(Warehouse access only)

Having read, understood and acknowledged the contents of the privacy notice provided pursuant to Article 13 GDPR and 5 PDPL, I hereby authorize the processing of my personal data for the following purposes:

A. to the processing of personal data performed by ISS (data controller) for the purpose of Internal access control activities (control of the security and integrity of corporate assets, as provided in point 12 above)

☐ **I Consent** ☐ **I do not consent**

Having read and understood the above information, I acknowledge that the processing of personal biometric data is strictly necessary to obtain access to ISS's warehouses areas, regarding of ISS's economic activities and initiatives, which is primarily centered around the transportation of goods that are routinely dispatched through the warehouses.

place, date Signature

_____ _____