The objective of this procedure is to implement the necessary processes to observe the requirements of the European Regulation (GDPR 2016/679) and Italian privacy law (decree D. Lgs 196/03.)
Roiatti has its own GDPR Manual that is currently being prepared, and will be reviewed at least annually and updated when necessary according to the laws/regulations. All procedures below described are also found in better details on the above-mentioned Manual.
As used herein information, personal information and data shall be construed as being privacy data within the meaning of the definitions in article 4 of cited law decree.

Management

Protection of data is the responsibility of all Roiatti management, administrative, warehouse, crew members and suppliers.
Management is responsible for establishing privacy policies and procedures which are documented herein. Specifically management will provide needed definitions, document, communicate and assign privacy data accountability using this procedural document.
Roiatti Srl defines “Data” as any document or information pertaining to and provided by Clients/AgentsEmployees//other third parties (both original and copies, either prinetd or electronic form).
The persons in charge of Data (Privacy) protection Management will be the Managing Director and the designated Internal DPO, Data Protection Officer.
Protection of privacy data by Roiatti Srl will be afforded to all categories of data which are from time to time defined and required to be protected by applicable laws and codes.
Currently privacy data consists of the following four (4) categories as defined in article 4 – Definitions – of cited law above:

a. “personal data”, any information pertaining to a physical person, identified or identifiable, even indirectly, by reference to any other information, including a personal identification number;
b. “identifying data”, personal data which permits the direct identification of a person;
c. “sensitive data”, personal data capable of revealing the race and ethnical origin, religious, philosophical, or other types of beliefs, political opinions, adhesion to party, union, associations or organizations of a religious, philosophical, political o union character, and personal data that discloses the state of health and sexual life.
e. "judicial data", personal data that can disclose the measures referred to in Article 3, paragraph 1, letters a) to o) and r) to u), of Presidential Decree November 14, 2002, n. 313, relative to criminal records, the list of sanctions for administrative offenses and related charges, or as an accused or suspected person under Articles 60 and 61 of the Code of Criminal Procedure).

Only the minimum sensitive data required by host nation laws or public entity regulations (example: customs) and GDPR will be collected, stored, used or disclosed by Roiatti Srl.
No judicial data will be collected, stored, or used by Roiatti Srl as this data has no meaningful purpose for its activities.

<u>Purposes for obtaining, using, retaining or disclosing of data.</u>
Personal Data may be used as follows:
1. Employees:
Data on employees is necessary to comply with the formalities required by law, regulations and Community legislation concerning the administration of employees, such data will be processed on paper and/or magnetic, electronic, and similar media, and in any case using instruments that guarantee security and confidentiality.
2. Customer/client:

- the establishment or continuation of a business contractual relationship;
- To manage the business
- to comply with proper administrative procedures, civil, fiscal and other requirements of law/Government regulations;
- commercial and marketing statistics;
- to answer questions;
- to maintain and update a most frequently asked questions, proposals and communications database
- for eventual subscription to our newsletter whenever available;

Notice

In order to operate and provide services, Roiatti Srl requires the collection of the shipper's personal information. The electronic information will be saved in secured devices and the physical documents will be stored in designated locations. This information can then be forwarded to Suppliers/Agents. By Agent, Roiatti means companies meeting the FIDI FAIM Data (Privacy) Protection Management standard or other companies that agree to observe Roiatti Data (Privacy) Protection Management Policy even though they are not in the association. The information will be submitted to pertaining authorities to provide the service that the client demands.

Transmittal of data.

All e-mails and other correspondence with or transmitting data will include an appropriate statement concerning the confidentiality, restricted use to the intended addressee and notification concerning misdirection of the correspondence and warning against any type of further unintended processing of the contents.

Electronic Distribution of data.

The PEC e-mail is the preferred system whenever transmitting personal sensitive or judicial data using electronic means. The PEC system is the equivalent of certified mail return receipt.

Choice and Consent

By utilizing our service, the customers, agents and other parties authorize Roiatti Srl to obtain and use personal data including document or information pertaining to and provided by the client, agents or other third parties.

The interested party/owner of the data shall be provided an express choice concerning the consent or otherwise to the collection and use of data, to include disclosure.

If business is conducted through correspondence or in person, the owner shall be requested to complete enclosure 1 or 2 herein, as the case may be. These enclosures include a consent choice for completion by the data owner. The enclosures also inform the owner of the consequences if consent is not given (inability for Roiatti to properly conduct business with the customer).

Whenever possible and practicable in conducting business orally, inform the customer/client of the consent choice and that if consent is not given or failure to provide, even partially, requested data places Roiatti Srl in the impossibility to fulfill their requests as we cannot complete required processes and laws. The written consent shall be obtained as soon as possible thereafter.

Collection

Data is obtained orally (phone call) and in writing (e-mail / fax / documents).

Data is collected orally during the course of conducting business telephonically or in person (office visits) (e.g. requests for information, requests for quotation etc.).

Written data is collected during conduct of business through normal correspondence or using electronic means (e-mail, transfer applications –drop box, we transfer, CD's, tapes, USB, etc.)

Data shall be requested for each individual business transaction regardless of whether the data is already in our possession.

Use, Retention and Disposal

Roiatti Srl records data both in written (physical) and electronic form and will use these data to provide services that the clients or the agents require.

Roiatti Srl is using "Agyo", a secured on-line platform where to keep privacy/personal data. Only authorized personnel as indicated in the system is allowed to access the website by logging in with his/her credentials.

Written data is found in personnel files, customer service files, accounting files, reports and other documentation required by law, regulation, community legislation or governmental entities.

Signed Privacy Policies for single Customers are kept in their moving files. In case of Agents/Suppliers with which we have continuous contractual business relationships, their signed policies are kept as attachments to the contracts or in a dedicated section in Agyo.

Data obtained orally is normally reduced to written form subsequently placed in the above-mentioned files.

Electronic form of data is retained on the server or on individual PCs.

Electromagnetic recording of oral data is not required nor permitted at Roiatti Srl.

Employee and management personal data is maintained for the duration of employment or appointment and destroyed upon termination of employment or cessation of the appointment.

Customer/client personal data is maintained for the period as indicated in article 2220 of the civil code (10 years) and then destroyed or in any case according to the current financial Italian law.
All documents are destroyed in a manner to render impossible any subsequent restoration of the personal data or sensitive date. This is accomplished using means such as paper shredders or incinerators but in no way trash cans unless the documents are reduced to a form that impedes the reconstruction of the information that they initially contained.
Data stored on electromagnetic media shall be destroyed through permanent cancellation from the storage media. Back up data will likewise be deprived of availability of all personal data previously destroyed/cancelled.

Access

Only Roiatti Employees that are directly dealing with procedures requiring client data will be authorized to access client data. Data access will be limited to the purpose of the work activity only. Clients utilizing Roiatti Srl have right to access, change, rectify and cancel their personal data and to oppose or revoke consent for that purpose given in accordance to European GDPR.

Disclosure to Third Parties

Roiatti Srl can only disclose information to agents that meet the FIDI FAIM data protection management standards. Agents/Suppliers that are not in this association will have to sign the form that establishes the FIDI FAIM standard. All third party agents are responsible for the same standard of information protection as Roiatti is.

Security for Privacy

a. All physical forms of data shall be kept in appropriate types of filing media to the maximum extent possible and kept solely in designated areas that are constantly surveilled during normal operating hours. After duty hours these areas are subject to both electronic anti intrusion surveillance and detection supported by random intrusion detection patrols.
Areas where personal data is maintained will be indicated with appropriate cautionary signs.
Custody of this data is the responsibility of personnel assigned to perform the related duties as indicated in Agyo and those located in the vicinity of the storage location. Personnel other than those charged with administrative or management duties will be challenged as to their need to know personal data before they can access files or systems where personal data is kept.
Sensitive data will be kept under key and in the custody of the person responsible for the function. Access or disclosure of these sensitive data will only be permitted to management personnel and personnel with a verified need to know and necessary to perform specifically assigned duties/responsibilities.
b. Data stored on electronic media is protected from unauthorized access and disclosure through use of credential authenticating application (password) which permit passing an access screening procedure.
Sensitive data is further protected by being kept in directory folders that have a second authenticating control which permits access only to designated personnel maintained by the systems manager. Sensitive data will not be kept in electronic form in generic directory folders that do not have the secondary authenticating control.
c. Access to the warehouse where forwarding/storage data is evident requires authorized entry. Unescorted entry is authorized for Roiatti Srl employees and certain suppliers strictly for performance of assigned duties and services respectively. The warehouseman will maintain a list of authorized personnel for unescorted entry. All other personnel require escorted entry by the warehouse man or other authorized employee*.*
Physical access to warehouse and office is documented in W16.

Quality

At least once a year we conduct Internal Audits in matter of GDPR to make sure the Manual is up to date and that files are complete with relevant and accurate personal information. In case adjustments are needed, we take proper actions.

Monitoring and Enforcement

Monitoring and enforcemnt of the GDPR Manual, Privacy policy and procedure of Roiatti is the respnsibility of all personnel, but in particular the administrative personnel that as part of their duties obtain, use and maintain files with personal data.
During internal audits/inspections the applicability of this procedure shall be verified and reported to management. The verification process shall include examination of files for correspondence to the requirement herein established as well as electronic systems access/security.
The GDPR Manual, Privacy policy and procedure of this document shall be reviewed at least annually and updated as necessary. It shall also be reiterated to dependent personnel once a year on the bulletin board.
Complaints and disputes/Data breach
All complaints involving personal data will be directed/addressed to and handled by the Managing Director of Roiatti Srl.
Questions or escalations of this policy are to be communicated to the Managing Director. Serious breaches or privacy violations will be reported to the head of department immediately. The head of department / Managing Director must also report the data or privacy incident to the client and resolve the problem as soon as possible.
Any resulting disputes will be processed in accordance with European GDPR and Italian law decree 196/03 depending on the type of data involved in the dispute.

Available systems (where possible)

PCs and Servers
Agyo

References to other procedures/processes (where possible)

K12 Security
W7 Computer systems security
W16 Building Safety and Control
GDPR Manual

Distribution (any official copies over and beyond the original)

None

Enclosures

1. Employee Privacy Data Information and Consent – Italian Decree 196/2003 (bilingual)
2. Information and Consent pursuant to Italian Privacy Law Decree 196/2003 article 13 (bilingual)
3. Sample e-mail privacy notice (bilingual)
4. Web site Data protection policy and legal notes (bilingual)