MORETTO SPA

Supplier Security Policy

MORETTO S.p.a. works with qualified suppliers and partners that pay attention to Information Security. Whenever possible, it uses suppliers that have achieved ISO/IEC 27001 certification and ISO/IEC 27017 and 27018 guidelines, which ensure adherence to information security strategies and procedures, for the provision of its services. This applies to:

- Strategic suppliers (changing them has a large impact): AWS, Microsoft
- Important but not strategic suppliers (changing them has little impact): Google, Pentasecurity

When MORETTO S.p.a. uses other suppliers, it promotes information security through the submission of a document, called the "Charter of Information Security Principles", which regulates the security requirements applied by MORETTO S.p.a., and which is duly shared with suppliers and signed by them.

Annex. Charter of IS Principles for Suppliers

Supplier's Commitments

To guarantee high standards of information security to its Customers, MORETTO S.p.a. requires its suppliers to ensure:

- The **confidentiality** of information: i.e., information should only be accessible to those who are authorised.
- The **integrity** of information: i.e. protection of information against unauthorised or unintended changes.
- The **availability of** information: i.e., that authorised users can actually access the related information when they request it.
- The **authenticity** of information: that is, that the information has a reliable provenance.
- The **privacy** of information: i.e. that there is a guarantee of protection and control of personal data included in the information.

To this end, the supplier shall follow the general principles on information security management set out below:

- All access to computer systems is subject to an identification and authentication procedure. Information access authorisations are differentiated according to the role and duties each individual, so that each user can access only the information they need, and are periodically reviewed.
- The procedures in place for the secure use of company assets, information, and the management systems thereof must be respected.

- Awareness of information security issues must be encouraged for all personnel (employees, contractors and other eligible persons) from the moment of recruitment and throughout the employment relationship.
- To be able to handle Information Security incidents in a timely manner, the Supplier must promptly report any security issues.
- Without authorisation, the Supplier may not access the premises or the individual company areas where information is managed in order to ensure the security of the equipment.
- The Supplier shall undertake to ensure compliance with legal requirements and information security principles in relations with MORETTO S.p.a. and its customers.
- The Supplier shall take all appropriate actions to effectively deal with an unforeseen event, guaranteeing the restoration of critical services in such a time and manner as to limit negative consequences on the service provided to and by MORETTO S.p.a.
- Security aspects must be included in all phases of the supplier's activity.
- The Supplier shall ensure compliance with the provisions of the law, statutes, regulations or contractual obligations, and any requirements inherent to information security, minimising the risk of legal or administrative sanctions, significant loss, or damage to reputation.

Any Supplier who wilfully or negligently disregards the established security rules may be prosecuted in the appropriate court and in full compliance with legal and contractual constraints.

Processing of personal data in accordance with GDPR 679/2016, as amended.

General instructions on data processing

In order to ensure that processing is carried out in full compliance with the rules in force, we recall the provisions of Art. 5 GDPR 679/2016, namely that the personal data being processed must be:

- processed lawfully and fairly;
- collected and recorded for specified, explicit and legitimate purposes, and used in other processing operations in terms compatible with said purposes;
- exact and if necessary, updated;
- relevant, complete and not excessive in relation to the purposes for which they are collected and subsequently processed;
- kept in a form which does not permit identification for any longer than is necessary for the purposes for which they were collected and subsequently processed.

Operational procedures to be followed for data processing

In order to correctly carry out the processing operations subject to communication by MORETTO S.p.a., the Supplier shall comply with the following indications:

- store the processed data in places not accessible to unauthorised persons;
- do not leave work tools unattended and accessible to third parties;
- systematically file paper and digital media in the places provided for that purpose;
- carefully retain and not disclose the personal identification code and, above all, the password for accessing electronic tools.

Limits of permitted processing

In all cases, the Supplier shall strictly observe the limits below. The supplier:

- shall not, without prior authorisation, use the communicated data in any other way than as indicated above;
- shall not disclose the data communicated to you to third parties;
- shall store media and instruments containing personal data in such a way as to prevent them from being accessible to unauthorised persons;
- shall be authorised in advance by MORETTO S.p.a. as Data Controller, for any communication of data externally, which is not envisaged by the entrusted service;

The aforementioned prohibitions on disclosure and circulation remain in force even after the conclusion of the existing contract.

Confidentiality

Finally, during the performance of the assignment and also after the termination thereof, the Supplier shall maintain complete confidentiality on all information, whether confidential and/or proprietary, of which it has become aware. This information shall not be disclosed to third parties, either wholly or in part, either in written, verbal or graphic form, or on magnetic media or in any other form without the prior express authorisation of the Data Controller.

"Confidential and/or reserved information" means any information, data, drawing, knowledge, finding, patented or patentable, know-how and, in general, any news, of a technical, economic, commercial or administrative nature, as well as any drawing, document, magnetic media or sample of material or product marked "reserved" or "confidential" or in any case, even if not marked, but identified even verbally as such by the Data Controller, who communicates it to the service provider in connection with the fulfilment of its mandate.

ADDRESS: VIA DEL LAVORO, 30, 36027 - ROSÀ (VI) - ITALY
TEL. : (+39) 0424 539673
FAX. : (+39) 0424 539863
MAIL : info@morettogroup.com
WEB : www.morettogroup.com

Tax ID Code - VAT Number and Registration Number: 01980110249 of the Vicenza Companies Register
Company stock i.v. euro 2,000,000.00