Co.Import Srl.

DATA SECURITY AND PRIVACY COMPLIANCE STATEMENT

ISSUED BY: **Galli Data Service Srl** (Data Protection Officer)	APPROVED BY: **Rastal Group*** (Data Controller)
GALLI DATA SERVICE SRL Strada della Viggioletta, 8 29121 Piacenza C.F. e P.I. 01690860331	Via A. Calvi, 35 29015 Castel San Giovanni (PC) Italia Telef. 0523.883805 Fax 0523.881995 Web : www.rastal.it E-mail: info@rastal.it PEC : rastal.italia@legalmail.it Codice SDI : PLSZVIT P.IVA 01208020337 Magazzino / Spedizioni: Via S. Biagio – Tel. 0523.865454 29011 Borgonovo V.T. (PC) IL BICCHIERE: E non solo RASTAL Italia s.r.l.
.....	.....
(Stamp/Signature)	(Stamp/Signature)

** The term "Rastal Group" or "Group" means the companies: Rastal Italia Srl and CO.IMPORT Srl.*
The Rastal Group is to be considered connected to Vetreria di Borgonovo Group, whose lead company provides intercompany services. The Group, using a shared IT infrastructure, shares the same policies on data protection and privacy compliance. This Statement is issued by the external consulting company, Galli Data Service Srl, which holds the position of Data Protection Officer, for the lead company of the connected Group.

SUMMARY

© Rastal Group (any improper use is strictly prohibited)

1) Purpose of the Statement

The purpose of this Statement is to present the main items of data security and privacy compliance adopted by the Group. This Statement represents a summary, intended for the dissemination, of the Accountability Model, a document which contains detailed elements strictly considered for internal use. This statement is issued by the Data Protection officer, Galli Data Service Srl (a company specialized in regulatory consulting services), representing a third-party attestation, provided to stakeholders, to certify the data security and compliance requirements adopted by the Group. The Management is involved in respecting and implementing the commitments contained in this Statement, ensuring and periodically verifying that the Statement is documented, implemented, reviewed, improved and disseminated to all personnel.

2) General principles and objectives

"Data Security and Privacy Compliance" are integral parts of the Group assets, representing a primary value of the Group business and growth.

2.1) Data Security

The data to be protected consist of all the information managed by the Group. The lack of adequate levels of security can lead to damage to the Group image, lack of customer satisfaction, as well as economic and financial damage. Information therefore represents a heritage of great value and an asset to be protected, by adopting procedures and behaviors aimed at guaranteeing its security. The Group therefore intends to ensure:

- data confidentiality (the information must be accessible only by authorized persons);
- data integrity (protecting the accuracy, precision and completeness of information and the methods for processing it);
- data availability (only authorized users can access the information and related assets when they request it).

2.2) Privacy Compliance (the protection of personal data)

Personal data means all information attributable, directly or indirectly, to a natural person. The correct management and protection of personal data allows the Group to: provide services respecting an adequate quality standard; avoid the risk of incurring penalties related to the violation of current regulations; encourage the relationship with the stakeholders, through guarantees of reliability. The Group undertakes to:

- respect the identity, personality, dignity of each subject with whom it interfaces, as well as the personal sphere and private life of each one;
- protect the personal data of each individual;
- respect the fundamental freedoms in terms of privacy, also through the guarantee of legislative compliance (EU Reg. 2016/679 and Legislative Decree 196/2003, as amended and supplemented by Legislative Decree 101/2018);
- reduce the use of personal data to the minimum necessary to achieve the stated purposes;
- limit the processing of personal data only to those pertinent to specific, explicit and legitimate purposes, with methods, tools and retention limits proportionate to the purposes to be achieved;

© Rastal Group (any improper use is strictly prohibited)

- provide the data subject with up-to-date, easily accessible and understandable information and communications relating to the processing of their personal data;
- guarantee the correctness and reliability of the data processed, by verifying and updating them;
- guarantee the rights of the interested parties regarding privacy.

3) Roles and Responsibilities

3.1) Data Controller

Each company of the Group, in the person of the Board of Directors, holds the office of Data Controller, exercising decision-making power over the means and purposes of the processing. The Group has developed an integrated compliance system, based on the sharing of document formats, as well as on the use of shared IT infrastructures.

3.2) Data Protection Officer

Regardless of the effective cogency of the obligations referred to in articles 37-39 of the GDPR, the lead company of the connected Vetreria di Borgonovo Group has decided to appoint a Data Protection Officer (DPO). The DPO is an external consulting company (Galli Data Service Srl), specialized in regulatory consulting services. The DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. The DPO, on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices, guarantees the Data Controller adequate support, for a correct application of the GDPR and for the choice of adequate security measures.

3.3) Privacy Coordinators

The Group has decided to appoint two Privacy Coordinators within the connected Group staff, in order to ensure adequate coordination between the DPO and company operations:

- HR Manager (in order to manage the requirements that involve employees)
- IT Manager (in order to manage the requirements that involve IT System)

3.4) Data Processing authorized

The Group appoints as Processing Authorized any person who processes personal data, usually identified in employees an individual IT profile. The appointment document contains:

- scope of processing (activities, categories of data, purpose of processing);
- instructions for proper data processing (possibly accompanied by specific training plans).

3.5) External data processors and sub-processors

The Group appoints external data processors all the subjects to whom a processing activity is outsourced (ex: HR suppliers/consultants; administrative suppliers/consultants; ICT suppliers/consultants; ecc.). Only suppliers are chosen who provide adequate guarantees of reliability, in terms of data security and confidentiality. Data processors are required to make use of sub-suppliers who provide the same guarantees required of them. In the event that a Group company is appointed as Data Processor by an external Controller, it will comply with the instructions received.

© Rastal Group (any improper use is strictly prohibited)

4) Data Mapping and Risk-assessment

In order to correctly implement the principle of accountability, envisaged by Article 5 of the GDPR, the Group carries out the following activities:

- context analysis (mapping of significant context elements for data protection and privacy compliance, for example IT systems inventory, organization chart, ecc.);
- processing register (mapping of the activities of data processing);
- risk-assessment (identification of the risk of varying likelihood and severity for the rights and freedoms of natural persons);
- privacy by default and by design (identification of the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects);
- data retention (identification of the data retention period);
- data transfer (identification of any data tansfer outside the EU and related legal basis);
- lawfulness principles (identification of the legal basis of the processing).

The following table identifies the method adopted by the Group to classify the aforementioned elements (the completed tables are included in the GDPR Accountability Model).

PROCESSING ACTIVITY	**Name**			
	Description			
PROCESSING ELEMENTS	**Type of data**			
	Data subjects			
	Purpose of processing			
	Data retention			
SUBJECTS INVOLVED	**Authorized**			
	Data processors			
	Joint Controller			
	Dissemination			
	Extra UE transfer			
	Transfer legal bases			
PROCESSING TOOLS	**Repository**			
	Asset			
RISK ASSESSMENT AND DPIA	**SEVERITY**			
	LIKELIHOOD			
	RISK LEVEL			
	DPIA ANALYSIS			
COMPLIANCE PRINCIPLES	**Lawfulness of processing**			
	Privacy by design/default			
	Specific security measures			
FINAL EVALUATION		The data processing can start/continue (risk mitigated by security plan)	The data processing must be submitted to further impact assessments	The data processing must be submitted to Authority preliminar check
NOTE				

5) Security Measures

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing (as pointed out by GDPR, Art.32), the Group implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The following paragraphs provide detailed evidence on the security measures, based on security controls conforming with best industry standards such as ISO 27001:2013.

5.1) Identity Management and segregation of duties

The following authentication and authorization measures are implemented:

- access to user profiles takes place through an authentication system based on user and password;
- passwords are assigned by the IT System Administrators (Ads) and replaced on first use by the users;
- passwords are subject to complexity and periodic replacement criteria;
- each user is associated with an individual profile;
- access privileges to applications / network shares / data are segregated in relation to the job role;
- there is a procedure for activating/deactivating users, returning equipment, managing data;
- roles with special privileges (Ads) are clearly defined, assigned to a small number of trained users and monitored through log-management.

5.2) Perimeter security, networks, malware protection

The following security measures are implemented:

- computers and servers are protected by specific antivirus solutions (ESET Antivirus);
- network traffic is managed/protected by firewall (Kerio);
- the security devices are equipped with specific protections against ransomware and/or IDS/IPS/DLP solutions;
- webfiltering systems are adopted (Kerio Web Filtering) with blocking of risk categories;
- networks are segmented and DMZ are used for web-services;
- wireless networks are segmented (internal, guests, etc.) and protected by password, periodically replaced (every 6 months);
- specific control and security systems, as multi-factor authentication, are adopted for remote connections (vpn).

5.3) Computer and server security

The following security measures are implemented:

- users do not have admin privileges (allowing them to disable/bypass security settings, change general settings, install software) on computer;
- the systems activate session time-out (screen-saver with password) if the user remains inactive for a certain period of time (10 minutes);
- encryption systems are used for notebook memories;

© Rastal Group (any improper use is strictly prohibited)

- access to the server room is locked, allowed only with badge and monitored;
- there are security systems dedicated to the server room (fire prevention, flood prevention, electricity control, etc.);
- there are systems for securely deleting data or physically destroying memory in the event of disposal or re-use of devices containing personal data.

5.4) Applications, web-site, e-mail security

The following security measures are implemented:

- updates aimed at preventing vulnerabilities of operating systems and applications are regularly installed (patching);
- critical applications are equipped with specific further authentication and authorization systems;
- the web-applications and/or the website are equipped with SSL certificates;
- the databases of critical applications are encrypted;
- a reliability assessment is carried out for any cloud services (evidence on the placement of servers; adequate contractual guarantees, Service Level Agreement; evaluation aboutf the data to be stored in the cloud; etc.);
- e-mail is subject to authentication procedures, antispam solutions, secure transmission systems, back-up procedures, disabling procedures in case of termination of employment;
- vulnerability assessment / penetration test services are carried out by specialized third parties;
- continuos monitoring of IT security, performance and users activities is carried out by dedicated application (Safetica);
- log management systems are implemented for Ads access, internet access, vpn use, use of removable memories, etc.

5.5) Security of sharing tools (multifunctions, removable memories, cloud repositories)

The following security measures are implemented:

- security systems dedicated to the use of shared printers are adopted (eg: printing with PIN);
- security systems dedicated to the use of shared scanners are adopted (eg: sending scans by email);
- fax devices have been rationalized/reduced and brought back to traceable tools;
- removable storage units (e.g. USB sticks, optical units, external hdds, etc.) are checked automatically by security scan;
- secure file sharing systems are used (only monitored internal cloud drive is allowed).

5.6) Mobile-device security

The following security measures are implemented:

- the Sim-Card PIN is activated;
- the authentication procedures foreseen by the device are activated;
- pre-established session time-out times are set;
- MDM solution is used which allows to remotely locate / block / erase the device, manage authorized apps, activate an antivirus solution.

5.7) Back-up and restore systems

The following security measures are implemented:

- specific applications are used to set up an automatic back-up system for all company data;
- the backup systems provide evidence of the successful conclusion of the operations;
- dedicated storage devices are used (NAS);
- the backup copies are stored in locations suitably distant from the server room;

© Rastal Group (any improper use is strictly prohibited)

- the virtualization infrastructure is replicated in a back-up data center;
- there are documented backup, disaster recovery and business continuity procedures;
- on-demand and scheduled recovery activities are performed.

5.8) Organizational measures

The following security measures are implemented:

- there is an inventory of IT infrastructure and systems;
- a standard configuration of the systems and a procedure for requesting/performing changes are defined;
- there is a security incident management procedure (see also par.6);
- a web-platform dedicated to the management of the compliance system is used;
- adequate privacy notice is disclosed to all subjects who provide personal data (see also par.7.1);
- specific procedures / forms are adopted to guarantee the exercise of the rights of the interested parties (see also par.7.2);
- all subjects (internal and external) who process personal data are specially appointed and instructed (see also par.3).

5.9) Physical security

The following security measures are implemented:

- the main physical location is perimeter and equipped with secure accesses and controls;
- the assignment of access keys is controlled;
- visitors are registered and welcomed in special areas or rooms;
- the office is equipped with alarm systems and video surveillance;
- office entrances and doors are lockable and there are lockable cabinets / drawers;
- documentation containing critical data is kept in secure and separate media;
- critical hardware devices (e.g. signature tools, home-banking tokens, etc.) are stored in secure mode;
- the staff is trained on the correct management of documents and work spaces;
- workstations and monitors are oriented to prevent unauthorized visibility;
- the exposure of confidential data on the covers of the company filing cabinets or bulletin boards is avoided;
- the premises used for archives are adequately protected;
- shredders are used before disposing of paper containing critical data.

6) Data Breach

In compliance with the provisions of articles 33-34 of the GDPR, the Group documents any data breach (understood as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed).

The Data Breach Register contains:

- a description of the nature of the violation of personal data, including where possible the categories and the approximate number of persons affected by the violation and the categories and the approximate number of records of personal data concerned;
- a description of the likely consequences of the violation of personal data;
- a description of the measures taken or proposed to remedy the violation of personal data, including, where appropriate, measures to mitigate any adverse consequences.

If necessary, the Group promptly makes available the information contained in the register to the guarantor authority, to the interested parties and to the stakeholders involved.

© Rastal Group (any improper use is strictly prohibited)

7) Transparency Measures

The Group takes appropriate measures to provide any information referred to in Articles 13,14 (privacy information) and Articles 15-21 (data subjects rights) in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The informations are provided in writing, or by other means, including, where appropriate, by electronic means.

7.1) Privacy notice

The group makes available to interested parties, in the manner permitted by law, all the information referred to in Articles 13, 14 of the GDPR, including: details of the Data Controller and of the DPO, purposes and legal bases of the processing, the recipients or categories of recipients of the personal data, etc.

7.2) Data subject rights

The Group has developed a specific procedure to facilitate the exercise of data subject rights, under Articles 15-22 of GDPR: right of access, rectification, erasure, restriction, portability, opposition.

8) Checks and Updates

The following table identifies the methods for maintaining / updating the compliance system:

ITEMS TO BE UPDATED	REF. GDPR	TIMING
Data Breach Security incident management	Art.33 GDPR	• Immediate registration and evaluation • Notification within 72 hours (if necessary)
Privacy by design Management of new processes, new technologies, new data processing	Art.25 GDPR	• Before the start of processing
Privacy Impact Assessment (PIA) Management of critical processing	Art.35 GDPR	• Before the start of processing
Right of access Response to requests from data subject	Art.15 GDPR	• Within 1 month of request
Data collection from third parties Information management	Art.14 GDPR	• Within 1 month of request
Context Analysis Recording structural changes	Art.24 GDPR	• When necessary (in case of variations)
Data processing Register Insertion of new data processing	Art. 30 GDPR	• When necessary (in case of variations)
Risk-assessment Evaluation and periodic review	Art.32 GDPR	• Annual audit
Security plan verification Verification of effectiveness	Art.32 GDPR	• Annual audit
Authorization and instructions New employee designation	Art.29 GDPR	• Before the start of relationship
Data processor appointment New outosurcer designation	Art.28 GDPR	• Before the start of relationship

This Statement is made available to stakeholders and updated through its publication on the Group's website.

© Rastal Group (any improper use is strictly prohibited)