1.FIELD OF APPLICATION, PURPOSE AND RECIPIENTS

The Company undertakes to comply with laws and applicable regulations relating to the protection of personal data in the countries in which the company operates. This Policy establishes the basic principles with which the Company processes the personal data of consumers, customers, suppliers, business partners, employees and others and indicates the responsibilities of its company departments and employees during the processing of personal data. This policy applies to the Company and to companies that directly or indirectly controls, that carry out activities within the European Economic Area (EEA) or that process the personal data of subjects within the EEA. The recipients of this document are all employees, permanent or temporary, and all collaborators who work on behalf of the Company.

2. REFERENCE DOCUMENTS

- The Regulation (EU) 2016/679 of 27 April 2016 (hereinafter GDPR)
- Legislative Decree no. 196 of 30 June 2003 (Privacy Code) and subsequent amendments
- Data retention policy
- Guidelines for the list of data and the mapping of processing activities
- Description of the Role of Data Protection Officer
- Procedure for requesting access to data by the interested party
- Data protection impact assessment methodology
- Procedure for reporting a data breach
- SGI Manual

3. OBJECT AND PURPOSE

The GDPR establishes the rules for the protection of individuals with regard to the processing of personal data, as well as the rules for the free circulation of such data (Article 1).

4.MATERIAL SCOPE OF APPLICATION

The material scope of the Regulation includes:

- Personal data subject to fully or partially automated processing.
- Personal data contained in an archive or intended to be entered there.
- Outside the material scope are:
- Personal data used in the course of activities that do not fall within the scope of EU law.
- Personal data used in customs controls and for asylum and immigration procedures.
- Personal data used in connection with purely personal activities.
- Personal data used for crime prevention purposes, etc.

5. TERRITORIAL SCOPE OF APPLICATION

The Regulation applies:

- Personal data used in the course of activities that do not fall within the scope of EU law.
- Personal data used in customs controls and for asylum and immigration procedures.
- Personal data used in connection with purely personal activities.
- Personal data used for crime prevention purposes, etc.

6. DEFINITIONS

Compared to the Privacy Code (Legislative Decree n.196 of 30/06/2003) the definition of sensitive data and judicial data has been eliminated; now we talk about:

- To data controllers and processors in the Union, regardless of where the processing takes place.
- To data controllers and processors who are not resident in the Union when the processing activities concern:
- Goods or services, regardless of whether or not a payment is required. - Monitoring of the behavior of subjects within the EU.
- To data controllers not established in the Union, but in a place where the law of a member state applies.
- Special categories of personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data intended to uniquely identify a natural person, data relating to health or sexual life or sexual orientation of the person.
- Health data: personal data relating to physical or mental health of a natural person, including the provision of health care services, which reveal information relating to his state of health.
- Special categories of personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data intended to uniquely identify a natural person, data relating to health or sexual life or sexual orientation of the person.
- Genetic data: personal data relating to the inherited or acquired genetic characteristics of a natural person which provide unambiguous information on the physiology or health of that natural person, and which result in particular from the analysis of a biological sample of the natural person in question;
- Biometric data: personal data obtained from a specific technical treatment relating to physical, physiological or behavioral characteristics of a natural person that allow or confirm the unambiguous identification, such as the facial image or dactyloscopic data.
- The following definitions of terms used in this document are taken from the General Regulations on European Union Data Protection (GDPR):
- Personal Data: any information concerning an identified or identifiable natural person
- ("Interested"); identifiable is considered the natural person who can be identified, directly or indirectly, with particular reference to an identifier such as the name, an identification number, data related to location, an online identifier or one or more characteristic elements of his physical, physiological, genetic, psychic, economic, cultural or social identity.
- Data Controller (Owner): the natural or legal person, public authority, service or other
- body which, individually or together with others, determines the purposes and means of personal data processing.
- Responsible for data processing (Data Processor DP): the natural or legal person, public authority, service or other body that processes personal data on behalf of the Data Controller.
- Data Protection Officer (DPO): the natural person, society, public or private entity, association or body to which the owner entrusts specific and defined tasks of management and control of data processing, even outside its organizational structure. The designation of a DPO is mandatory:
- - if the processing is carried out by a public authority or by a public body;
- - if the main activities of the owner or manager consist of treatments that require regular and systematic monitoring of large-scale subjects; or - if the main activities of the owner or manager consist in the large-scale processing of particular categories of data or personal data relating to penal convictions and crimes.
- The mandatory designation of a DPO may also be provided for in further cases under the national law or EU right. When a DPO is designated on a voluntary base, the identical requirements apply - in terms of criteria for the designation, position and duties - that apply to the DPOs designated in mandatory way (Article 37 of GDPR).
- Treatment: any operation or set of operations, carried out with or without the aid of automated processes and applied to personal data or sets of personal data, such as collection, registration, organization, structuring, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, the comparison or interconnection, limitation, deletion or destruction.
- Consent of the interested party: any manifestation of free, specific, informed and unambiguous will of the interested party, with which the same expresses his / her consent, by means of a declaration or positive unequivocal action, that the personal data concerning him are being processed.
- Personal data breach: the security breach that accidentally or unlawfully involves the
- destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed.

- Anonymization: Irreversible de-identification of personal data in such a way that the person cannot be identified using reasonable times, costs and technologies by the Owner or any other
- person to identify the interested party. The data protection principles should therefore not apply to anonymous information, i.e. information that does not relate to an identified or identifiable natural person.
- Pseudonymization: the processing of personal data in such a way that the personal data can no longer be attributed to a specific subject without the use of additional information, provided that such additional information is kept separately and subject to technical and organizational measures to ensure that such personal data are not attributed to an identified or identifiable natural person. The pseudonymization reduces, but does not completely eliminate, the possibility of connecting personal data to the interested party. Since the pseudonymized data are however personal data, the processing of pseudonymized data should be compliant with the principles of personal data processing.
- Cross-border processing: processing of personal data that takes place in the context of activities of plants in more than one member State of a Data Controller or DP in the Union where the Data Controller or DP is established in more than one member State; or the processing of personal data that takes place in the context of activities of a single plant of a Controller or DP in the Union, but which affects or probably affects in a substantial way on subjects in more than one member State;
- Supervisory Authority: the independent public authority established by a member State pursuant to Article 51of the EU GDPR; for Italy it is the Guarantor for the protection of personal data (GUARANTOR) based in Piazza di Monte Citorio n. 121 - 00186 Rome - www.gpdp.it - www.garanteprivacy.it E-mail: garante@gsdp.it Fax: (+39) 06.69677.3785 Telephone switchboard: (+39) 06.69677.1

7. PRINCIPLES APPLICABLE TO THE PROCESSING OF PERSONAL DATA

The principles applicable to data protection outline the responsibilities of organizations in managing personal data. The Owner is competent for compliance with the principles, and must be able to prove it.

LAWFULNESS, FAIRNESS AND TRANSPARENCY

Personal data must be processed lawfully, correctly and transparently towards the subject.
Processing is lawful only if and to the extent that at least ONE of the following conditions is met:

- The interested party has given consent for one or more specific purposes.
- The processing is necessary for the execution of a contract of which the interested party is a party.
- The processing is necessary to fulfill a legal obligation of the data controller.
- The processing is necessary for the safeguarding of the vital interests of the subject.
- The processing is necessary for the execution of a task of public interest or connected to the exercise of powers vested in the data controller.
- The processing is necessary for the pursuit of the legitimate interest of the data controller.

LIMITATION OF PURPOSES

Personal data must be collected for specific, explicit and legitimate purposes, and subsequently processed in a way that is not incompatible with these purposes.

DATA MINIMIZATION

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are treated. The company must apply anonymization or pseudonymization to personal data, if possible, to reduce the risk to those concerned.

ACCURACY

Personal data must be accurate and, if necessary, updated; all reasonable steps must be taken to promptly delete or rectify inaccurate data with respect to the purposes for which they are processed.

LIMITATION OF THE STORAGE PERIOD

The data must be kept in a form that allows the identification of subjects for a period of time not longer than the achievement of the purposes for which they are processed.

INTEGRITY AND CONFIDENTIALITY

Taking into account the technologies and other security measures available, the cost of implementation and the probability and severity of risks to personal data, the Company has implemented technical and organizational measures to ensure a level of adequate security for personal data, including protection from accidental or unlawful destruction, loss, modification, disclosure or unauthorized access.

RESPONSIBILITY

The Data Controller is competent to comply with the principles described above and is able to prove it through the correct application and observation of this policy.

8. PRINCIPLES OF DATA PROTECTION IN BUSINESS ACTIVITIES

The Company has implemented the principles of data protection in its privacy management system, guaranteeing the regulatory compliance of the various operational phases, from collection to treatment.

NOTIFICATION TO THE INTERESTED PARTIES

(See chapter Guidelines on Proper Treatment.)

CHOICE AND CONSENT OF THE INTERESTED PARTY

(See chapter Guidelines on Proper Treatment.)

COLLECTION

The Company's goal is to adopt and constantly improve its organizational and operational processes to collect as little personal data as possible. If personal data is collected by third parties, the controller must ensure that personal data is legally collected. Privacy Organizational Model Manual pursuant to Regulation (EU) 2016/679 Rev. 01 of 14/09/2018 DOCUMENT FOR INTERNAL USE Page 13 of 44

USE, STORAGE AND DISPOSAL

The purposes, methods, registration limit and retention period of personal data must be consistent with the information contained in the Privacy Policy. The company must maintain accuracy, integrity, confidentiality and the relevance of personal data based on the purpose of the processing. Appropriate security mechanisms must be used to protect personal data to prevent it from being stolen, misused or abused and prevent personal data breaches. The Owner is responsible for compliance with the requirements listed in this section.

DISCLOSURE TO THIRD PARTIES

Whenever the Company uses a supplier or third party business partner for the processing of personal data for its account, it is necessary to obtain guarantees that it provides security measures to safeguard personal data adequate to the associated risks (for example inappropriate use of personal data, unauthorized disclosure, etc.).

The Company undertakes to contractually request the supplier or business partner to provide an adequate level of data protection (GDPR-NRET Form Nomination of External Data Processor). Suppliers or business partners must process personal data only to fulfill their contractual obligations towards the Company or behind Company instructions and not for other purposes. When the Company processes personal data jointly with a third independent party, it must explicitly specify its own responsibilities and those of the third party in the relevant contract or in any other legally binding document.

CROSS-BORDER TRANSFER OF PERSONAL DATA

The Company does not carry out transfers of personal data abroad, however possibly before transferring personal data from the European Economic Area (EEA) appropriate protective measures must be used, including the signature of a data transfer agreement, as required by European Union and, if necessary, the authorization of the relevant Data Protection Authority must be obtained.

RIGHT OF ACCESS BY INTERESTED PARTIES

The company is responsible to provide to interested parties a reasonable access mechanism to allow them to access their personal data and must allow them to update, rectify, delete or transmit their personal data, where applicable or required by law. The access mechanism will be further detailed in the access application Procedure to data by the interested party.

DATA PORTABILITY

Interested parties have the right to receive, upon request, a copy of the data they have provided to us in a structured format and to transmit such data to another Data Controller, free of charge. The company is responsible for ensuring that such requests are processed within one month, are not excessive and do not affect the rights relating to personal data of other persons.

RIGHT TO BE FORGOTTEN

Upon request, interested parties have the right to obtain by the Company the cancellation of their personal data if one of the following reasons exists:

- Personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
- The interested party revokes the consent on which the treatment is based and there is no other legal basis for the treatment.
- The interested party opposes the processing and there is no legitimate overriding reason to proceed with the treatment.
- Personal data have been unlawfully processed.
- Personal data must be deleted to fulfill a legal obligation.

9. GUIDELINES ON CORRECT TREATMENT

Personal data must be processed only if explicitly authorized by the Data Controller. The Owner establishes whether to perform the Data Protection Impact Assessment for each data processing activity based on the Data Protection Impact Assessment Guidelines.

COMMUNICATIONS TO INTERESTED PARTIES

At the time of collection or prior to the collection of personal data for any type of processing activity, but not limited to the sale of products, services or marketing activities, the Data Controller is responsible for adequately informing interested parties in the following:

- the identity and contact details of the Data Controller;
- if appointed, the identity and contact details of the Data Protection Officer (DPO);
- methods and purposes of data processing;
- legal conditions for data processing;
- categories of recipients;
- potential data transfers (if any);
- the retention period;
- the rights of the interested party regarding his personal data;
- whether the data will be shared with third parties and the security measures established by the Company to protect personal data;
- the consequences of not consenting to the processing.

This information is provided through the Privacy Policy (GDPR-IC Model for Customers; GDPR-IF for Suppliers). Furthermore, in compliance with the principle of Accountability (responsibility), the company will have to obtain confirmation from the interested party that he has read and understood the content of the policy by means of a specific declaration on the copy thereof.

OBTAIN CONSENTS

Whenever the processing of personal data is based on the consent of the interested party, or on other legitimate reasons, the Data Controller is responsible:

- of the conservation of a registration of this consent (by keeping the policy form signed by the interested party);
- to provide the interested parties with the options to give consent;
- to inform the interested parties and guarantee them how the given consent can be revoked at any time (every time the consent is used as a legal basis for processing).

Where the collection of personal data refers to a minor under the age of 16, the Data Controller must ensure that the consent of the holder of parental responsibility is provided prior to collection using the specific form.
When requesting to correct, modify or destroy personal data records, the Data Controller must guarantee that such requests are handled within a reasonable amount of time and must also record the requests and keep a register of these. Personal data must be processed only for the purposes for which they were originally collected.
In case the Company wishes to process personal data collected for another purpose, the Company must request consent to interested parties in clear and concise written form. Any such request should include the original purpose for which the data were collected and also the new or additional purposes. The request must also include the reason for the change of purpose. Now and in the future, the Data Controller must ensure that the collection methods comply with the law, good practices and relevant industry standards. The Owner is responsible for the creation and maintenance of a register of Privacy Policies.

TREATMENT OF SPECIAL CATEGORIES OF PERSONAL DATA

It is forbidden to process personal data that reveal:

- race;
- ethnic background;
- political opinions;
- religious beliefs;
- philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data;
- health data;
- sexual life of a person;
- sexual orientation.

Exceptions: the interested party has given his explicit consent;

- The processing is necessary to fulfill the obligations and exercise the specific rights of the data controller or of the interested party in matters of labor law and social security and social protection, to the extent which is authorized by Union or member States law or by a collective agreement under the law of Member States, in the presence of appropriate guarantees for the fundamental rights and interests of the interested party;
- the processing is necessary to protect a vital interest of the interested party or of another natural person if the interested party is physically or legally incapable of giving his / her consent;
- the processing is carried out, in the context of its legitimate activities and with adequate guarantees, by a foundation, association or other non-profit organization that pursues political, philosophical, religious or trade unions purposes, provided that the treatment only concerns members, former members or persons who have regular contacts with the foundation, association or organization for its purposes and that personal data are not communicated externally without the consent of the interested party;
- personal data are manifestly made public by the interested party;
- the processing is necessary to ascertain, exercise or defend a right in court or whenever the judicial authorities exercise their judicial functions;
- the processing is necessary for reasons of significant public interest on the basis of Union or Member States law, which must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for appropriate and specific measures to protect fundamental rights and interests of the interested party;
- the treatment is necessary for purposes of preventive medicine or occupational medicine, evaluation of the employee work capacity, diagnosis, assistance, health or social care or management of systems and health or social services on the basis of Union or Member State law or in accordance with the contract with a healthcare professional;
- processing is necessary for reasons of public interest in the public health sector, such as protection from serious cross-border threats to health or the guarantee of high standards of quality and safety of health care and medicines and medical devices, on the basis of Union or members States law which provides for appropriate and specific measures to protect the rights and freedoms of the interested party, in professional secrecy in particular;
- the processing is necessary for archiving purposes in the public interest, for scientific or historical research or for statistical purposes.
- Lawfulness of processing is a prerequisite.

10. REQUIREMENTS FOR THE PROCESSING OF EMPLOYEE PERSONAL DATA

Any processing of personal data of employees by departments and individuals within the Company must take place for a legitimate purpose and must meet the following requirements.

COMMUNICATION TO EMPLOYEES

For the purposes of transparency in the processing of employee personal data, when a department or individual within the Company collects the personal data of an employee, the employee must be informed of the types of data collected, of the purposes and types of processing, the employee's rights and the security measures adopted to protect personal data. This information is provided by a specific policy on the processing of personal data (GDPR-ID form).

COMMUNICATION TO CANDIDATES

The same transparency guaranteed for the processing of employees' personal data is also ensured for the collection of personal data of a candidate being interviewed for a possible recruitment. The candidate must be informed of the types of data collected, of the purposes and types of processing, his rights and the security measures adopted to protect personal data. This information is provided by a specific policy on the processing of personal data (GDPR-ICL form).

CHOICE AND CONSENT OF EMPLOYEES

In principle, the Company may process the personal data of employees for legitimate purposes as an employer and it can generally do so without obtaining the employee's consent, to improve the efficiency of internal operations.
Safety and human resource management activities such as interviews, recruitment, termination of the employment relationship, attendance, compensation and benefits, employee services, health and occupational safety may result in treatment of sensitive personal data.

COLLECTION

Corporate departments and individuals must collect employee personal data for legitimate purposes and must respect the principle of Data Minimization. If the personal data of a job candidate or of an employee are collected by a third party (for example temporary employment agencies), the Company must do everything possible to ensure that this third party obtains the personal data by legitimate means. No company department or individual can collect personal data of candidates or employees in a way that does not comply with the law or business ethics.

USE, STORAGE AND DISPOSAL

Company departments and individuals must use, store and dispose of employee personal data in a manner consistent with the communication to the employee. They must also ensure its accuracy, integrity and relevance. The company has put in place adequate security measures to protect the personal data of employees from accidental or unlawful destruction, loss, modification, unauthorized access or disclosure, in accordance with the security policy of information and other documents describing data security. Company departments and physical persons must not destroy or unlawfully modify the personal data of employees.
They must not access, sell or supply unlawfully or without authorization, employee personal data to third parties. In the course of business operations, the Data Controller will decide whether the personal data of employees will be processed in the following ways to minimize the risk for the data protection: the personal data of employees can be anonymized for the purpose of irreversible de-identification; or the data can be aggregated into statistical or research results. (The principles of processing personal data do not apply to anonymized data and aggregate data as they are not personal data).

DISCLOSURE TO THIRD PARTIES

When business departments and individuals need to disclose employee personal data to a supplier, a business partner or third party, they must try to ensure that the supplier, business partner or other third party provides security measures to safeguard employee personal data that are adequate for the associated risks. They should also require the third party to provide the same level of data protection that they provide to the Company by contract or other agreement (GDPR-NRET form). Additionally, when company departments and individuals disclose personal data of the employees in response to a request from law enforcement or a judicial authority, they must first inform the Data Protection Officer (DPO) who is authorized by the Company to make a coordinated effort to handle the request.

CROSS-BORDER TRANSFER OF EMPLOYEE PERSONAL DATA

The company does not carry out cross-border transfers of data, however if it is necessary to do so, before transferring personal data, company departments and individuals must consult the Data Protection Officer (DPO) or the Data Controller to determine if cross-border transfer is necessary and legitimate.

ACCESS OF EMPLOYEES

Company departments must provide employees with reasonable means to access personal data held about them and allow employees to update, correct, delete or transmit their personal data if necessary or required by law. When responding to an employee access request, company departments cannot provide any personal data until they have verified the identity of the employee. The company must make sure to know the identity of the person making the request before it can send personal data to the person himself.

RESPONSIBILITY

The Human Resources Department is responsible for managing the protection of employees' personal data.

11. COMPANY ORGANIZATION

The GDPR introduces new organizational obligations. The responsibility to ensure adequate processing of personal data is up to anyone who works for or with the Company and has access to personal data processed by the Company; to this aim the Company has implemented its own Privacy organization chart.

The main areas of responsibility can be identified in the following organizational roles:

- the Data Controller, he makes decisions and approves the general strategies of the Company regarding the protection of personal data. That role is covered by the legal representative pro-tempore.
- The Data Protection Officer (RPD / DPO),he is responsible of the management of the personal data protection program and is responsible for the development and promotion of the personal data protection policies from beginning to end, as defined in the Description of the Manager's Role of Data Protection.
- The system administrator, he is responsible for:
- ensure that all systems, services and equipment used for data recording meet acceptable security standards.
- Conduct regular checks and scans to ensure that security hardware and software are functioning correctly.
- Internal Audit, he is responsible for internal audits aimed at complying with the procedures and policies on protection of personal data.
- Authorized persons, employees formally authorized to carry out processing operations from holder.

12. GENERAL OBLIGATIONS

REGISTERS OF PROCESSING ACTIVITIES

The Data Controller must keep a register of processing activities containing the following information:

- • contact details of the Data Controller and, where applicable, of the joint Data Controller and of the Data Protection Officer;
- • purpose of the treatment;
- • categories of interested parties;
- • categories of personal data processed;
- • categories of recipients to whom the personal data have been or will be disclosed;
- • where applicable, the transfers of personal data to a third country or an international organization;
- • where possible, the deadlines set for the cancellation of the various categories of data;
- • where possible, a general description of the technical and organizational security measures.

RESPONSE TO PERSONAL DATA VIOLATION INCIDENTS

When the Company becomes aware of an alleged or actual violation of personal data, the Data Controller assisted by DPO must perform an internal investigation and take appropriate corrective measures in a timely manner, according to the Data Breach Response and Reporting Procedure.

AUDIT AND RESPONSIBILITY

Internal Audit is responsible for verifying how company departments implement this policy. Any employee who violates this Policy will be subject to disciplinary actions and may also be subject to civil or penal liability if his conduct violates laws or regulations.

CONFLICTS WITH THE LAW

This policy is intended to comply with the laws and regulations of the place of plant and of the countries in which the Company operates.