DATA PROTECTION POLICY

FOREWORD

Reference legislation

The European Parliament and Council approved the EU Regulation No. 679/2016 on the protection of Personal Data (hereinafter referred to as "GDPR" and "Regulation"), which came into force on 25 May 2016 and is directly applicable throughout the European Union as of 25 May 2018 with the consequent repeal of Directive 95/46/EC of the European Parliament and Council of 24 October 1995, transposed in Italy by Legislative Decree No. 196 of 30 June 2003 (Personal Data Protection Code).

The GDPR fundamentally changes privacy legislation and in particular:

- harmonises the regulations on the protection of Personal Data within the entire European Union;
- attaches fundamental importance to the principles of accountability, privacy by design and privacy by default;
- in line with the principle of accountability, introduces, inter alia, the institutions of the register of processing operations, data protection impact assessment and data breach notification;
- strengthens and introduces new rights of data subjects, which companies are required to guarantee in order to ensure that the processing of Personal Data is carried out in full compliance with the law, also to increase the level of services provided to customers;
- introduces the figure of the Data Protection Officer;
- tightens the administrative fines which, in the case of the most serious violations, may reach a maximum of €20,000,000 or 4% of the global annual turnover at the level of a business group.

Subject matter and purpose

This Policy on the Protection of Personal Data sets out the guidelines to which the "Data Controller" must adhere when planning and carrying out any activity involving the processing of Personal Data in order to ensure the protection of such Data in accordance with the requirements of the relevant legislation and in particular with Regulation (EU) 2016/679 on the Protection of Personal Data ("GDPR").

The provisions of this Policy are designed to ensure that personal data are processed with respect for the fundamental rights and freedoms and dignity of natural persons. In particular, the Policy identifies:

- the addressees of the privacy legislation;
- the general principles for the protection of Personal Data in business activities;
- the procedures for updating and reviewing the Policy;
- the main roles envisaged in the field of privacy;
- the necessary activities that the Data Controller must apply in order to be adequate for the processing of Personal Data.

General Principles

The Data Controller carries out its activities in compliance with the general privacy principles set out in the relevant legislation and in this Policy. In particular, in planning or carrying out any activity involving the processing of Personal Data, the Data Controller shall ensure that Personal Data are:

- processed in a lawful, fair and transparent manner towards the data subject (principle of lawfulness, fairness and transparency);
- collected for specified, explicit and legitimate purposes, and subsequently processed in a way that is not incompatible with those purposes (purpose limitation principle);

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (principle of data minimisation);
- accurate and, where necessary, timely updated in relation to the purposes for which they are processed (principle of accuracy);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed (principle of limited storage);
- processed in a manner that ensures adequate security of Personal Data, including protection, by appropriate technical and organisational measures, against unauthorised or unlawful processing and accidental loss, destruction or damage (integrity and confidentiality principle).

Definitions

As defined by law and for the purposes of this Policy, the following definitions apply:

- **"Special Categories of Personal Data":** personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data intended to uniquely identify uniquely identify a natural person, data relating to a person's health or sex life or sexual orientation - Article 9 GDPR;
- **"Data breach":** a security breach that accidentally or unlawfully results in the destruction, loss, alteration, unauthorised disclosure of or access to Personal Data transmitted, stored or otherwise processed; in the event of a Personal Data breach, the data controller must notify the breach to the competent supervisory authority without undue delay and, where possible, within 72 hours of becoming aware of it, unless the breach is unlikely to present a risk to the rights and freedoms of natural persons. Where the personal data breach is likely to present a high risk for the rights and freedoms of natural persons, the controller shall also notify the data subject of the breach without undue delay;
- **"Personal data":** any information relating to an identified or identifiable natural person ("data subject"),
  - "Identification data": those that allow direct identification. By way of example, identification data are: name, signature/signature, photograph, address, private address, work address, lP and Mac Address telephone number, telefax or e-mail number; identity card number, passport, driving licence, social security or welfare position number; car registration number, tax code and other personal identification numbers (health cards);
  - "Personal characteristics data": marital status data, family data (minors, dependent children, etc.), date and place of birth, physical characteristics (height, weight, etc.), gender, nationality, mother tongue; physical data
  - "Data of social circumstances": housing characteristics, position with respect to military obligations, preferences and lifestyle, membership of clubs, associations, licences, permits, social profiles, etc., authorisations
  - "Education, professional, work and career data": education, educational qualifications, curriculum vitae, professional experience, membership of professional associations, information on suspension or termination of employment or change of employment, company/administration to which you belong, category/grade, job, work history, public offices held
  - "Business information data": activities and shops, business licences, subscriptions to publications/media, artistic, literary, scientific, technical creations, orders, shipping vouchers, invoices; articles, products, services; contracts, agreements, transactions
  - "Economic-financial data": income, annuities, investments, assets, credits, loans, endorsements, bank data (accounts, etc.) pension plans, economic data of the assignment, insurances, mortgages, subsidies, benefits, credit history, credit cards. - "Transaction data": goods and services provided by

the data subject, goods and services received by the data subject, financial transactions, fees/compensation.

- **"Data Protection Officer or DPO":** means the person designated by the Data Controller or Data Processor to perform support and control, advisory, training and information functions in relation to the application of the GDPR;
- **"Garante":** the Italian Data Protection Authority;
- **"Data processor":** the natural person authorised to carry out processing operations by the Data Controller or Data Processor;
- **"Limitation of processing":** the marking of Personal Data stored with the aim of limiting its processing in the future - Article 4(3), GDPR;
- **"Accountability Principle":** the principle that requires the controller to put in place appropriate technical and organisational measures to ensure and to demonstrate that processing is carried out in accordance with the provisions of the GDPR taking into account the nature, scope, context and purposes of the processing, as well as risks having different probability and severity for the rights and freedoms of natural persons;
- **"Privacy by default principle":** the principle that requires the controller to put in place technical and organisational measures to ensure that, by default, only the Personal Data necessary for each specific purpose of the processing is processed, for example, by reducing the amount of data collected, the scope of the processing, the storage period and the number of individuals who have access to the Personal Data;
- **"Principle of Privacy by Design":** the principle that requires the controller to adopt, both when determining the means of processing and at the time of processing itself, appropriate technical and organisational measures to ensure compliance with the GDPR and the protection of the rights and freedoms of data subjects;
- **"Profiling":** any form of automated processing of Personal Data consisting of the use of such Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects of that natural person's professional performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements - Article 4(4), GDPR;
- **"Procedure":** the document adopted by the Controller in order to govern specific internal processes;
- **"Privacy Contact Person":** the person within the Controller's company who supports the DPO in performing his functions.
- **"Register of processing operations":** data controllers and processors must keep the register of processing activities carried out under their responsibility, containing the information referred to in Article 30 GDPR;
- **"Controller":** the natural or legal person, public authority, service or other body that processes Personal Data on behalf of the Controller - Article 4(8) GDPR;
- **"Data Controller":** the natural or legal person, public authority, service or other body which alone or jointly with others determines the purposes and means of the processing of Personal Data; where the purposes and means of such processing are determined by Union or Member State law, the Data Controller or the specific criteria applicable to its designation may be determined by Union or Member State law - Article 4(7), GDPR. For the purposes of this Policy, the Data Controller is the Company;
- **"Processing"** means any operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure

by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction - Article 4(2), GDPR;

Scope of application

All employees, consultants with coordinated and continuous collaboration contracts, occasional external collaborators, maintenance staff, interns and other collaborators of the Data Controller in various capacities are required to scrupulously comply with this Policy within the scope of their respective competences and activities. In order to ensure that all recipients are aware of the principles, guidelines and procedures adopted by the Data Controller in compliance with this Policy, this Policy and its updates are included and shared in the data processing documentation.

PRIVACY ROLES

2.1 Privacy Contact Person

The Privacy Contact Person may be identified by the Data Controller from among the 'appointees', who have specialised skills in the protection of Personal Data.

2.2 Data Processors

The Data Controller adopts internal procedures for appointing as Data Processors the natural persons authorised by it to process Personal Data and for updating such appointments. The Controller also ensures that Data Processors are adequately trained through courses and the provision of precise instructions on how to carry out processing. To this end, the Controller organises training events/activities on the protection of Personal Data, the applicable legislation and the privacy framework adopted. These training events/activities are organised periodically and, in any case, should significant regulatory or organisational changes occur.

2.3 External Data Processors (Articles 27 and 28 GDPR)

The Data Controller may outsource certain processing to parties identified as Data Processors, selected taking into consideration their ability to offer sufficient guarantees to implement technical and organisational measures adequate to comply with the requirements of the GDPR. Whenever a processing operation is outsourced to a natural or legal person, the Data Controller shall ensure that such third party is appointed as External Processor in compliance with the provisions of the GDPR. Once the External Processor has been selected in compliance with this Policy, a contract or other legal deed of appointment is signed that contains all the elements required by the GDPR, including precise instructions to be followed by the External Processor and the right of the Controller to terminate the contract in the event of default by the other party.

Throughout the contractual relationship, continuous monitoring is ensured through periodic checks on the work of the External Managers in order to ascertain compliance with privacy legislation and the instructions given by the Controller. To this end, reports may be requested, questionnaires may be filled in and/or inspections may be carried out at the External Manager's premises, also involving, where necessary, IT experts. Should criticalities emerge and should they persist or be of such a magnitude as to justify the termination of the contractual relationship, the Controller shall terminate the contractual relationship with the External Manager. In the event of the appointment of a new External Manager or the modification of existing External Managers, the Processing Register must also be updated accordingly. The operational details for the management of external Processors are described in the specific Procedure.

PROCESSING MANAGEMENT

3.1 Conditions of lawfulness of processing (Articles 5 and 6 GDPR)

The Data Controller ensures that Personal Data are processed only where one of the conditions of lawfulness of processing provided for by the GDPR is met, taking into consideration the nature of the personal data being processed (i.e. common data, special categories of Personal Data, judicial data and data of minors). In particular, the Data Controller adopts the necessary safeguards to ensure that Personal Data are processed only where at least one of the following conditions applies:

- the data subject has given his/her consent;
- processing is necessary for the performance of a contract to which the data subject is party or for the performance of pre-contractual measures taken at the data subject's request;
- processing is necessary for compliance with a legal obligation;
- processing is necessary in order to safeguard the vital interests of the data subject or another natural person;
- processing is necessary to pursue a legitimate interest of the data controller or a third party, unless the interests or the rights and freedoms of the data subject prevail.

The Controller provides the direct sellers who interact with the data subjects with the necessary instructions to ensure compliance with the law and this Policy. Where the basis of lawfulness of the processing is consent, the direct sellers must issue a notice to the data subjects and request their consent, in compliance with internal procedures and instructions received, before the processing begins. Consent must be free, specific and informed, manifested by an unequivocal affirmative action and requested separately for each purpose of the processing. Internal legislation establishes the obligation to record the consent obtained through procedures that ensure easy retrieval of the date, manner and content of the consent. The terms of the processing, indicated on the notices, contain and describe in a precise manner the period of retention of Personal Data or, if this is not possible, the criteria used to determine this period.

3.2 Processing of data of minors and of particular categories of personal data (Articles 8 and 9 GDPR)

In the event that the processing is based on consent and concerns personal data of minors, the Data Controller ensures that the processing takes place exclusively if this consent is given or authorized by the holder of parental responsibility. The consent or authorization of the holder of parental responsibility is recorded through processes that ensure easy recovery. If the processing concerns particular categories of personal data and the processing is based on consent, the Data Controller ensures that information is issued to the interested parties and requested explicit consent, in compliance with the internal procedures, before the processing begins.

3.3 Precautions to be taken by the Representative

The permanence of documents and paper documents with the Person in Charge must be limited to the time strictly necessary to carry out the processing operations; at the end of the activity the documentation must be placed in the respective archive. In the case of output documents (meaning as such documents or media containing Personal Data produced and released by the structure to subjects external to the structure itself) it is necessary, upon delivery or sending, to verify that the person receiving the document is entitled to withdrawal and use. The Representative must treat any product of the processing of Personal Data, even if it does not constitute a definitive document (notes, interrupted printouts, test prints, temporary processing prints, etc.) with the same precautions that would be reserved for the definitive version.

3.4 Management of the Processing Register (Art. 30 GDPR)

The Data Controller manages the keeping, updating and conservation of the Processing Register in compliance with the legislation and this Policy. The company functions involve the Privacy Contact in the evaluation phase of activities that could lead to a modification or institution of a treatment and the possible need to update the Register of treatments, including by way of example:

- the planning of a new initiative involving the processing of Personal Data;
- the extension of a processing already foreseen to new categories of interested parties or Personal Data;
- any change to the organizational structure of the company;
- the signing of supply contracts that lead to the appointment of the counterparty as external manager;
- the categories of recipients to whom the Personal Data being processed are communicated;
- the need to transfer the Personal Data processed outside the European Union;
- any modification to the information systems adopted;
- the adoption of new technical and/or organizational measures.

The updated Processing Register must be made available to all the Data Controller's representatives in a manner designed to ensure easy consultation.

PRINCIPLES OF PERSONAL DATA PROTECTION

4.1. Accountability (Art. 5 GDPR)

In order to process Personal Data in accordance with current legislation and this Policy, the Data Controller adopts adequate technical, organizational and security measures, as well as adequate mechanisms to control the constant compliance of such measures over time with continuous and constant updating. The Data Controller documents the activities carried out to ensure that the processing is carried out in compliance with the applicable legislation and keeps this documentation available for any access by the Guarantor.

4.2 Privacy by design (Art. 25 GDPR)

The Data Controller implements adequate technical and organizational measures, such as pseudonymisation, aimed at effectively implementing data protection principles, such as minimisation, and integrating the necessary guarantees into the processing in order to satisfy the requirements of this regulation and protect the rights of interested parties

4.3 Privacy by default (Art. 25 GDPR)

The data controller implements appropriate technical and organizational measures to ensure that, by default, only the personal data necessary for each specific processing purpose are processed. This obligation applies to the amount of personal data collected, the scope of processing, the retention period and accessibility. In particular, these measures ensure that, by default, personal data are not made accessible to an indefinite number of natural persons without the intervention of the natural person.

5. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS (Articles 44, 45, and 46 GDPR)

The transfer of Personal Data outside the European Union can take place only in the presence of at least one of the conditions listed below:

- an adequacy decision by the European Commission;
- standard data protection clauses adopted by the European Commission;
- contractual clauses between the Data Controller and the Owner/Manager recipient of the Personal Data in the third country approved by the supervisory authority;
- adoption of a code of conduct or certification mechanism and contextual commitment of the Owner/Manager recipient of the Personal Data to apply the appropriate guarantees.

The transfer of Personal Data to a third country or an international organization will also be possible in the event that:

- the interested party has explicitly given consent after having been informed of the possible risks;
- the transfer is necessary for the execution of a contract concluded between the interested party and the owner or of pre-contractual measures adopted at the request of the interested party;
- the transfer is necessary for the conclusion or execution of a contract stipulated between the owner and a third party in favor of the interested party;
- the transfer is necessary for important reasons of public interest.

6. RIGHTS OF INTERESTED PARTIES

The rights attributed by the GDPR to interested parties are divided into two categories: (i) rights that require an express request from the interested party; (ii) the rights to which the legislation links an obligation of the owner independently from the receipt of a prior request from the interested party.

6.1 Rights subordinate to an express request from the interested party (Articles 15-21 GDPR)

The process for managing the rights exercised by interested parties through express request can be traced back to the following main phases:

- receipt of the request;
- management of the request;
- feedback to the interested party and archiving.

The main rights that the GDPR guarantees to the interested party and which the same can exercise upon request are the following:

1. Right of Access. The interested party has the right to obtain confirmation from the data controller as to whether or not personal data concerning him or her are being processed and, in this case, to obtain access to the personal data which includes the personal data provided by the interested party. the observable Personal Data generated in execution of the contract, the terms of processing including the expected retention period.

2. Right of Rectification. The interested party has the right to obtain from the data controller the rectification of inaccurate personal data concerning him without unjustified delay.

Taking into account the purposes of the processing, the interested party has the right to obtain the integration of incomplete Personal Data, also by providing a supplementary declaration;

3. Right of Cancellation. The interested party has the right to obtain from the data controller, if the reasons indicated by the GDPR exist, the deletion of the Personal Data concerning him or her without unjustified delay and the data controller has the obligation to delete the Personal Data without unjustified delay;

4. Right to restriction of processing. The interested party has the right to obtain from the data controller the limitation of processing when the hypotheses provided for by the art. 18 of the GDPR;

5. Right of Opposition / Revocation. The interested party has the right to oppose, or withdraw consent, at any time, for reasons related to his particular situation, to the processing of Personal Data concerning him pursuant to Article 6, paragraph 1, letters e) or f) of the GDPR, including profiling. The data controller shall refrain from further processing the Personal Data unless he demonstrates the existence of compelling legitimate reasons to proceed with the processing which prevail over the interests, rights and freedoms of the interested party or for the assessment, exercise or the defense of a right in court.

6. Right to Portability. The interested party has the right to receive the Personal Data concerning him or her provided to a data controller in a structured, commonly used and machine-readable format and has the right to transmit such Data to another data controller without impediments from part of the data controller to whom it was provided if the processing is carried out by automated means. Finally, in the case of exercise of the rights of rectification, cancellation and/or limitation of processing by the interested party, the Data Controller will also provide the communication to the interested recipients provided for by Article 19 GDPR.

6.2 Rights not subordinate to a request from the interested party

Even in the absence of a request from the interested party, the Data Controller guarantees that suitable information is provided to the same at the time of collection of his Personal Data from the same or, if the Data is not collected directly from the interested party, within the following deadlines:

- within a reasonable period of obtaining the Personal Data, but at the latest within one month, taking into account the specific circumstances in which the Personal Data are processed;
- in the event that the Personal Data are intended for communication with the interested party, at the latest at the time of the first communication to the interested party;
- if communication to another recipient is envisaged, no later than the first communication of the Personal Data.

7. SECURITY MEASURES (Art. 32 GDPR)

The Data Controller adopts the appropriate technical and organizational measures to guarantee a level of security adequate to the risk, taking into account the state of the art and implementation costs, the nature, object, context and purposes of the processing, as well as the risk of varying probability and severity for the rights and freedoms of natural persons.

9. DATA BREACH (Articles 33 and 34 GDPR)

If a violation of Personal Data occurs, the technical and organizational measures adopted must still be able to recognize and counteract the violation. In the event that a violation of Personal Data occurs that presents a risk to the freedoms and rights of the interested parties, the Data Controller provides an immediate reaction method that allows:

- notification of the violation to the Guarantor without unjustified delay and, where possible, within 72 hours of becoming aware of it and, if the conditions are met, to the interested party;
- the adoption of the measures necessary to mitigate the negative effects of the violation.

The Data Controller keeps a register of violations and establishes internal procedures that govern its updating as each violation occurs, regardless of the risk presented for the rights and freedoms of the

interested parties, and mechanisms for storing all communications regarding the violation. This register indicates all the elements required by applicable legislation, including:

- the circumstances surrounding the breach;
- the consequences;
- the measures adopted to combat it and limit its effects;
- the Personal Data involved; adequate information to allow the Data Controller to determine the reasons for not having made the notification, or having made it late.

10. ATTACHMENTS

This Policy is supplemented by the documents attached below: Annex 1: Appointment Management Procedure

Annex 2: Paper Document Management Procedure

Annex 3: Electronic Instrument Management Procedure

Annex 4: Procedure for the Management of the Rights of Interested Parties

Annex 5: Mail and IT Network Management Procedure

Annex 6: Data Breach Management Procedure