



Group Privacy Policy

2023

Version date:
May 2023





This Policy sets out rules and guidelines for the management of personal data processing, in accordance with the provisions of European Regulation (EU) no.2016/679 (GDPR) and the local regulations that govern this matter, by Lavazza Group member companies subject to the application of the GDPR.

| Release | Date | Description | |
|----------------------------|-------------|--|--|
| V. 3 | May 2023 | <i>First release: November 2018 Second release: October 2020 Third release: May 2023</i> | |
| ISSUING DEPARTMENT: | | <i>Policies, Guidelines and Procedures</i> | |
| PROCESS OWNER: | | <i>DPO</i> | |
| VERIFIED BY: | | <i>Legal, Corporate Affairs & Compliance</i> | |
| | | <i>HR</i> | |
| | | <i>IT</i> | |
| | | <i>Internal Auditing</i> | |
| APPROVED BY: | | <i>CEO</i> | |

CONTENTS

| | |
|---|-----------|
| 1. INTRODUCTION | 4 |
| 2. GENERAL PRINCIPLES..... | 9 |
| 2.1 INTRODUCTION | 9 |
| 2.2 DEFINITION OF PERSONAL DATA | 10 |
| 3. PRIVACY ORGANISATIONAL MODEL (P.O.M.) | 11 |
| 3.1 INTRODUCTION | 11 |
| 3.2 ROLES WITHIN THE LAVAZZA GROUP | 11 |
| 3.3 DATA CONTROLLER | 12 |
| 3.4 DATA CONTROLLER REPRESENTATIVE | 12 |
| 3.5 DATA PROCESSOR (GROUP COMPANIES AND THIRD PARTIES) | 13 |
| 3.5.1 Group member companies | 13 |
| 3.5.2 Third Parties..... | 14 |
| 3.6 DATA PROTECTION OFFICER | 14 |
| 3.7 PRIVACY COMMITTEE | 15 |
| 3.8 PRIVACY FOCAL POINT OF THE LAVAZZA GROUP MEMBER COMPANIES | 15 |
| 3.9 INTERNAL CONTACT PERSONS OF THE LAVAZZA GROUP MEMBER COMPANIES | 15 |
| 3.10 AUTHORISED PROCESSORS | 16 |
| 3.10.1 CCTV Footage Authorised Processors..... | 17 |
| 4. REGISTER OF PROCESSING ACTIVITIES | 17 |
| 5. MANAGEMENT MODEL | 17 |
| 5.1 COLLECTION..... | 18 |
| 5.1.1 Purposes..... | 18 |
| 5.1.2 Legal Basis | 18 |
| 5.1.2.1 Consent..... | 18 |
| 5.1.2.2 Contract performance..... | 20 |
| 5.1.2.3 Fulfilment of a legal obligation..... | 20 |
| 5.1.2.4 Legitimate interest | 20 |
| 5.1.3 Privacy Notice | 21 |
| 5.2 PROCESSING – GENERAL PRINCIPLES | 21 |
| 5.2.1 Processing carried out by Third Parties | 22 |
| 5.2.2 Cross-border transfer of personal data – intra-group flows | 22 |
| 5.2.3 Cookies and similar technologies..... | 23 |
| 5.2.4 Security | 24 |
| 5.3 SPECIFIC PROCESSING: TERMINATION OF THE PROCESSING - ERASURE AND DESTRUCTION | 24 |
| 6. RIGHTS OF THE DATA SUBJECT AND HANDLING OF REQUESTS | 25 |
| 6.1 RIGHT OF ACCESS | 25 |
| 6.2 RIGHT TO RECTIFICATION..... | 25 |
| 6.3 RIGHT TO ERASURE | 26 |
| 6.4 RIGHT TO RESTRICTION OF PROCESSING | 26 |
| 6.5 RIGHT TO PORTABILITY OF THE DATA | 26 |
| 6.6 RIGHT TO OBJECT | 26 |
| 6.7 HANDLING REQUESTS AND TIME LIMITS FOR RESPONDING | 27 |
| 7. OPERATING INSTRUCTIONS | 27 |
| 8. PRIVACY BY DESIGN & BY DEFAULT | 27 |



| | |
|--|-----------|
| 9. DATA PROTECTION IMPACT ASSESSMENT (DPIA) | 28 |
| 10. DATA TRANSFER IMPACT ASSESSMENT (TIA) | 29 |
| 11. NOTIFICATION IN THE EVENT OF A PERSONAL DATA BREACH | 29 |
| 12. INSPECTIONS BY THE DATA PROTECTION AUTHORITY | 30 |
| 12.1 RULES OF CONDUCT DURING INSPECTIONS..... | 31 |
| 13. TRAINING | 31 |
| 14. AUDITS | 32 |
| 15. PENALTIES | 32 |

1. Introduction

Scope and purpose

This Policy applies to LUIGI LAVAZZA S.p.A. (hereinafter, also “Parent Company”) and/or its Italian and foreign subsidiaries (hereinafter referred to individually as “Company” or “Subsidiary” and collectively as “LAVAZZA Group”) subject to the provisions set out in the GDPR in the processing of personal data (as defined hereafter in paragraph 2.2) during the performance of business activities.

The purpose of this document is to regulate personal data processing within the LAVAZZA Group so as to guarantee full compliance with the provisions laid down in European Regulation no. 2016/679 (GDPR).

Responsibilities

All the Managers of the Group are responsible for ensuring compliance with this Policy. In particular, all the parties involved in the processing of personal data must contribute to the protection of personal data by applying this Policy and the “Privacy Principles” described below.

This Policy may be implemented and supplemented, where necessary, following instructions from the Corporate Affairs & Compliance Department of the Parent Company LUIGI LAVAZZA S.p.A. and the Group’s Data Protection Officer (DPO).

PRIVACY PRINCIPLES

Processing and purposes

The LAVAZZA Group processes personal **data lawfully, correctly and transparently**, for the achievement of **specified, explicit and legitimate business purposes** and adopts reasonable measures to ensure that the personal data is **accurate** and, where necessary, **kept up to date**.

Third parties

Third Parties (suppliers, business partners and consultants) that for any reason whatsoever enter into a business relationship with LAVAZZA Group companies, and, by virtue of this, undertake personal data processing operations on behalf of the latter, are appointed as **Data Processors** and are contractually required to comply with the measures for the security and confidentiality of the data, as well as to refrain from any use or disclosure that is not authorised by the LAVAZZA Group.

The LAVAZZA Group places particular importance on the protection of the **confidentiality** of personal data, asking all employees and collaborators, internal and external, to contribute to the achievement of this objective.

Communication of personal data

The personal data provided may be **disclosed** to third parties in order to comply with legal obligations, to respect orders issued by public authorities, or to enforce or defend a legal claim, and, within the context of the companies forming the LAVAZZA Group, to meet business requirements or internal administrative purposes, including the processing of the personal data of customers and employees.

Personal data may be communicated to third parties, in their capacity as independent Data Controllers or Data Processors, with the **consent** of the Data Subjects, if required by law, and in any event after providing sufficient information on the purposes of the processing. Personal data is not **disseminated**.

Retention

Personal data is retained solely for the **time necessary** to achieve the purposes for which it was collected and in compliance with the time limits laid down by the law or required to enforce a legal claim. Personal data is stored in compliance with the Group’s

Retention Policy, which is made available to the employees in the company Intranet, in the [Our Privacy - Policy & Procedure](#) section, unless local regulations provide for different storage requirements.

Employment relationships

With reference to the data that the company processes within the framework of **employment relationships**, the LAVAZZA Group uses personal data only for the achievement of connected purposes (such as, for example, compliance with employment relationship conditions, payroll, benefits, tax, social security and welfare obligations, health and safety in the workplace; training and career development activities, performance evaluation; use of personal data, including photographs and videos for company purposes).

Commercial activities and marketing

In compliance with the principles of **lawfulness, correctness and transparency**, and, if required by law, with the **consent** of the data subjects, the LAVAZZA Group may process personal data for the achievement of business and marketing purposes (such as, for example: sending out advertising material and other promotional and marketing initiatives; direct sales activities; analysis of consumer habits and choices; and statistical processing).

Security

The LAVAZZA Group uses **secure technology and takes every reasonable precaution to protect personal data** from undue disclosure, alteration or improper use. The protective measures put in place are aimed, in particular, at reducing to a minimum the risk of destruction or loss, whether accidental or deliberate, of the data, as well the risks of unauthorised access or processing that is not permitted or is non in keeping with the purposes for which it was collected.

Within the Group, regular **risk analysis** activities are carried out in order to check compliance with the defined security standards and, where necessary, adopt new security measures following organisational changes and technological innovation or changes in type of data collected. Implementation of the security measures is **constantly monitored and periodically verified**.

Self-assessment

The LAVAZZA Group performs a **periodic self-assessment** in order to verify that this Policy is applied to the entire Group and that all the people within the Group comply with these *Principles*.

Compliance

In the definition of the Privacy Principles, the LAVAZZA Group complies with European Regulation no. 679/2016 and, in general, with the applicable laws and regulations that protect the confidentiality of personal data in the jurisdictions in which LUIGI LAVAZZA S.p.A. or its subsidiaries operate. Specific jurisdictions may require the LAVAZZA Group to supplement this Policy in order to comply with local laws.

Contact

For any questions and/or doubts concerning the application of this Policy, please contact the **DPO of the LAVAZZA Group** (privacyDPO@lavazza.com) or the **Corporate Affairs & Compliance Department** of the Parent Company.



Glossary

In order to facilitate the understanding of this document, a list of key words and their definitions is provided below:

- **System Administrator:** natural person entrusted with the management and/or maintenance of an IT and data processing system or of some of the hardware and software components thereof, as defined in the General Provision of the Italian Data Protection Authority of 27 November 2008 and its subsequent amended versions;
- **Supervisory Authority (or Authority):** the Authority provided for in article 51 of the GDPR, i.e., one or more independent public authorities entrusted by a Member State with the task of monitoring the application of the Regulation in order to protect the fundamental rights and freedoms of natural persons in relation to personal data processing. In Italy, the independent supervisory authority is the Data Protection Authority (the so-called “Privacy Guarantor”);
- **Authorised Processor:** natural person authorised to physically carry out personal data processing on behalf of the data controller. All employees who process personal data within the scope of their employment duties are authorised processors;
- **Standard contract clauses:** a safeguard tool defined by the European Commission to regulate and legitimise the transfer of personal data outside the European Economic Area;
- **Privacy Committee:** group responsible for coordinating the application of the privacy policy established within the Parent Company and composed of representatives from the relevant HQ departments (HR, Internal Audit, Legal and Corporate Affairs, ICT, Digital Marketing, Marketing and others identified on a case-by-case basis);
- **Communication:** the communication of personal data to one or several parties other than the data subject, by the representative of the data controller or the data processor not established within the territory of the European Union, by the persons authorised to process the personal data under the direct authority of the data controller or the data processor, or by persons expressly appointed to do so, in any form, also by making the data available, or through consultation or through interconnection;
- **Subsidiary:** all the companies directly or indirectly controlled by Luigi LAVAZZA S.p.A.
- **Data Processing Agreement (“DPA”):** data processing agreement entered into by a data controller and a data processor to regulate the scope, purposes and methods of processing, as well as the obligations and responsibilities of the parties;
- **Data Protection Impact Assessment (“DPIA”):** assessment of possible risks presented by personal data processing and the impact that the occurrence of the risks identified may have on the rights and freedoms of data subjects;
- **Data Protection Officer (or “DPO”):** the person designated by the data controller or by the data processor to provide support and control, advice, training and information on the application of the Regulation. The DPO cooperates with the

Authority and is the point of contact, also for data subjects, for issues relating to the processing of personal data;

- **Identification Data:** the identification data is the data that can be used to obtain the direct identification of the data subject. For example, the identification codes, including those derived from registry data (e.g., tax code) and the unique codes attributed to a person based on pre-defined criteria (e.g., customer code), are identification data ;
- **Personal data:** any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, by reference to any other information, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- **Sensitive/special category data:** Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or membership to trade unions, genetic data and biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;
- **Data Controller Representative:** natural person appointed by the data controller to perform the activities aimed at guaranteeing constant and strict compliance with the laws in force concerning personal data processing, as well as to represent the data controller in dealings with the data subjects and the Authorities and in all third-party appointment contracts and deeds;
- **Disclosure:** the communication of personal data to unspecified parties, in any form, also by making it available or available for consultation;
- **Privacy Focal Point ("PFP"):** natural person appointed within each subsidiary as the point of contact between the subsidiary itself and the Group DPO, with the task of facilitating the management of all the local issues and specific aspects of personal data processing;
- **General Data Protection Regulation ("GDPR"):** the "General Data Protection Regulation", namely (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, which establishes European rules for the protection of personal data;
- **LAVAZZA Group:** Luigi LAVAZZA S.p.A. and its subsidiaries;
- **Headquarters ("HQ"):** the registered office of Luigi LAVAZZA S.p.A.;
- **Data Subject:** the natural person directly or indirectly identified or identifiable by an item of personal data and, in any event, the person the data processed relates to;
- **Legitimate Interest Assessment: ("LIA"):** balance between the interests of the data controller that processes the personal data on the basis of its legitimate interest and the rights and freedoms of the subjects the personal data processed relates to;

- **Luigi LAVAZZA S.p.A. (or Parent Company):** the parent company with registered office in Via Bologna no. 32 - Turin (Italy); the registered office is also referred to as the Headquarters (“HQ”);
- **Privacy Organizational Model (“P.O.M”):** set of rules, procedures, organizational and technical measures adopted to ensure compliance with the regulations on the protection and privacy of personal data;
- **Internal Contact Person:** natural person who supports the data controller in ensuring the proper management and assessing the conformity of the personal data processing carried out within his/her department;
- **Data Processor:** the party (natural or legal person) appointed as data processor for the processing of personal data carried out on behalf of the data controller, as a result of a formal deed of appointment that defines the scope of duties assigned to the person;
- **Sub-Processor:** a party (natural or legal person) who carries out data processing operations on behalf of the data controller;
- **Data Controller:** the natural or legal person that determines the purposes and means of the processing of personal data. The data controller also has the task of ensuring the implementation of technical and organisational measures ensuring a level of security appropriate to the risk presented by the processing;
- **Transfer Impact Assessment (“TIA”):** assessment of the impact of transferring personal data outside the EU and the EEA where the appropriate guarantees for the transfer as set out in Chapter V of the GDPR are not in place;
- **Transfers of personal data:** any transfer of personal data, which is undergoing processing or is intended for processing after transfer to a third country outside the EU/EEA for which an adequacy decision has not been issued, including onward transfers of personal data from one third country to another.
- **Processing:** any operation or set of operations performed without making use of electronic instruments, for the collection, recording, organisation, storage, consultation, processing, alteration, selection, retrieval, comparison, use, interconnection, blocking, disclosure, dissemination, deletion or destruction of personal data, including data not recorded in a database;
- **Data breach:** a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2. General Principles

2.1 Introduction

European Regulation no. 2016/679¹, better known by its acronym GDPR (*“General Data Protection Regulation”*), is a regulation of the European Union on the **protection of natural persons with regard to the processing of their personal data**, aimed at regulating the privacy rights of European citizens in a consistent manner.

These rules were created in order to **increase the trust of data subjects**, making them more aware of how their personal data is used and enabling them to make an informed decision as to whether or not to consent to its use².

This has a considerable impact on the data that is normally collected and managed by the company within the context of its normal business, marketing and operating activities, as a consequence of the **raising of the level of protection of personal data** - concerning customers and consumers, in addition to employees and partners - implemented by the Regulation.

Within the context of the performance of its business activities, the LAVAZZA Group collects a significant quantity of confidential data and information, which it undertakes to process in compliance with all the laws on privacy and confidentiality in force in the jurisdictions in which it operates.

In particular, in the principles set out in the **Code of Ethics of the LAVAZZA Group** it is stated *“We are committed to protecting any sensitive, confidential and proprietary information regarding the Group. Confidentiality is essential to ensure trust and authenticity, both within the Group and in our dealings with partners and consumers”*.

The same confidentiality commitment during the use, processing and safekeeping of data must be undertaken and guaranteed by all employees and anyone else who, in the exercise of their activities, process personal data on behalf of the LAVAZZA Group.

Employees and partners of the LAVAZZA Group, at all levels, are therefore required to recognise if they are collecting, using, processing, storing or sharing the personal data being protected. Hence, they must be informed and aware of the **key principles that regulate the processing of personal data**, namely that the data:

- must be processed **lawfully, correctly and transparently** in relation to the data subject, in compliance with the specific purposes described in a clear and intelligible form in the privacy notice and on the basis of the requirements of lawfulness that justify its processing (including express consent to the processing, where necessary);
- must be collected for **specified, explicit and legitimate purposes** and further processed in ways not incompatible with these purposes (*“Principle of purpose limitation”*);
- must be **adequate, relevant and limited** to what is necessary in relation to the purposes for which it is being processed (*“Principle of minimisation”*);
- must be **accurate** and, where necessary, **kept up to date**;
- must be stored in a form that permits the identification of the data subjects **for no longer than is necessary for the purposes** for which it is processed (*“Principle of storage limitation”*);
- must be processed in a way that ensures the **appropriate security** of the personal data, including protection - using appropriate technical and organisational measures - against unauthorised or

¹ Following the coming into force of the GDPR, Legislative Decree no. 101/2018 on *“Provisions on the adaptation of national legislation to the provisions of Regulation (EU) 2016/679”* was issued on 10 August 2018, for purposes of coordination with pre-existing Italian laws.

² The aim of the GDPR is to provide a higher level of protection concerning the processing of personal data carried out: (i) by **Data Controllers operating in the territory of the EU/EEA, regardless of whether the processing takes place in the Union or not**; (ii) by **Controllers established outside the EU/EEA, but manage the data of European consumers, offering products and services within the territory of the EU (regardless of whether or not there is a correlated payment)**.

unlawful processing and from loss, destruction, alteration, unauthorised disclosure or access that may cause any damage.

Compliance with these principles is the responsibility of the **Data Controller**, supported by the Data Protection Officer (DPO), and involves the **assessment, management and ongoing monitoring of possible risks**.

The Privacy Contact Person (Internal Contact Person) of each Group member company, as defined below in paragraph 3.9, **has the task of ensuring compliance with this Policy in his/her area of responsibility**.

All employees/partners of the LVAZZA Group are responsible for compliance with the principles and rules defined in this document.

Compliance with the provisions set out this Policy is to be considered an essential part of the contractual obligations of employees/partners.

Any breaches of this Policy may result in **disciplinary action**, including - in the most serious cases - dismissal, in accordance with the laws in force and the national labour agreements, or the termination of the collaboration relationship (for third parties).

Compliance with the provisions of law on the protection of natural persons with regard to the processing of personal data, in addition to being an approach in line with the principles set out in the Group's Code of Ethics and correlated documents, also constitutes an **important opportunity for rationalising, classifying and sorting the personal data stored by the company according to updated criteria of necessity and security, limiting excess data duplication and avoiding the risks presented by the processing thereof**.

2.2 Definition of personal data³

Personal data means **any information relating to an identified or identifiable natural person ("data subject")**; an identifiable natural person is one who can be identified, **directly or indirectly**, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier⁴ or to one or more elements specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person⁵.

³ The GDPR does not apply to the processing of personal data in connection with the exercise of a **purely personal or household activity**.

⁴ Online identifiers produced by devices, applications and tools (such as IP addresses, cookies, identification tags, etc.) may leave tracks that, if combined with unique identifiers and other information received from the server, may reveal the identity of natural persons. Digital identification of the data subject is also included therein, through authentication mechanisms (such as the same credentials used by the data subject to access - *log in* - the online service offered by the Data Controller).

⁵ The GDPR does not apply to the processing of **anonymous information**, namely: (i) information, which does not relate to an identified or identifiable natural person; (ii) personal data rendered anonymous in such a manner that the Data Subject is no longer identified or identifiable. The Regulation does not apply to the processing of anonymous information for statistical or research purposes.

3. Privacy Organisational Model (P.O.M.)

3.1 Introduction

This paragraph explains the **roles** established and actively involved in the management of the **Privacy Organisational Model (P.O.M.)** within the LAVAZZA Group and the **responsibilities** for applying the Model in the various organisational structures.

The main figures involved in the personal data processing management model are:

- **Data Controller**
- **Data Controller Representative**
- **Data Processor** (Group Companies and Third Parties) and possible Sub-Processors
- **Data Protection Officer**, local and of the Group
- **Privacy Committee**
- **Privacy Focal Point** of the Group Member Companies
- **Internal Contact Persons** of the Group Member Companies (First and second level)
- **Authorised Processors.**

3.2 Roles within the LAVAZZA group

Taking into account Group's self-assessment activity performed on type of personal data processed, intra-group processing, organisational processes, and technological safeguards - it is considered that, **in general and subject to exceptions, the Main Establishment⁶, where Group guidelines concerning the processing of personal data are made, is the registered office (HQ) of the Parent Company, LUIGI LAVAZZA S.p.A., i.e., the company identified as the "lead authority"⁷ for Data Protection issues.**

It is at the registered office, in fact that the principles and the rules to be followed in processing personal data, within the Group and irrespective of whether or not the data is processed at that office, are actually defined and shared⁸.

Although the general guidelines on the processing of personal data are provided by the Parent Company, the roles and responsibilities of each Company in relation to the processing of personal data taking place within each organisation have been defined locally.

In particular, the Group member companies can process personal data acting in the capacity of Data Controllers or of Data Processors on the basis of ad hoc agreements on the processing of personal data (the so-called "**Framework Agreements**") aimed at regulating - in the context of **intra-group relationships** - the nature, purpose, duration of processing, type of personal data, categories of data subjects, obligations and rights of the parties.

In its capacity as lead company, Luigi Lavazza S.p.A. identifies from among the managers reporting directing to the Managing Director the **first level "Internal Contact Persons"** who are responsible for identifying and

⁶ Under art.4, point 16 of the GDPR and the Guidelines for the identification of the lead supervisory authority adopted on 5 April 2017 by the Article 29 Working Party (Art. 29 WP).

⁷ Along the same lines, art.2.1.2 of the Guidelines on the identification of the lead authority adopted on 5 April 2017 by the Article 29 Working Party states that "if processing is carried out by a group of undertakings whose HQ is located in the EU, it is assumed that the establishment of the parent company is the decision-making centre with regard to personal data processing and, therefore, is to be considered the main establishment of the group".

⁸ In this connection, see Recital 36 of the GDPR.

appointing the **second level "Internal Contact Persons"** within their departments and according to a cascade process.

As for the other Group member companies, each manager in charge of one of more subsidiaries ("General Manager"/"Regional Director") identifies the **first level "Internal Contact Persons" at each Subsidiary**.

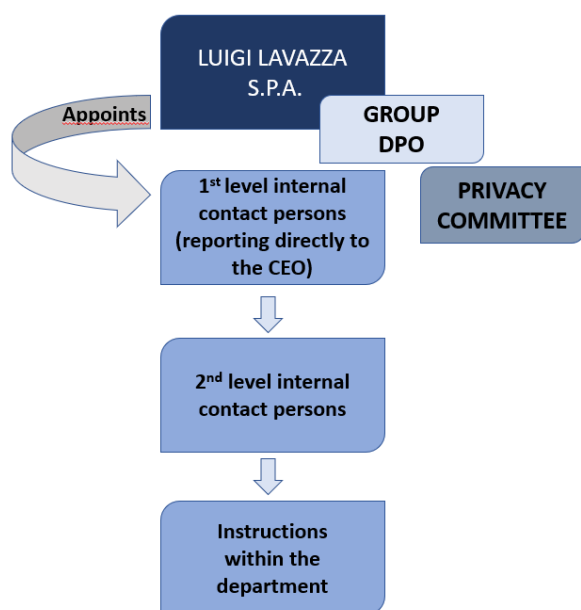
3.3 Data Controller

The **Data Controller is the natural or legal person that, either alone or jointly with others determines the purposes and means of the processing of personal data**. The Group Companies acting as Data Controllers have been identified on the basis of this definition.

The title may refer to all personal data processed by the subsidiary (employee/collaborator data, customer and consumer data) or to part thereof (only employee/collaborator data or only customer and consumer data).

In particular, each Subsidiary is the Data Controller for personal data relating to the management of its employees/collaborators, whereas for personal data relating to customers and consumers, the Subsidiaries may act as Data Controller or as Data Processor based on specific intra-group agreements entered into between them (the so-called "**Framework Agreements**").

Organisation of Lavazza's HQ



3.4 Data Controller Representative

The Data Controller, in the person of his/her legal representative *pro tempore*, may decide, under his/her own responsibility and within the framework of the organisational set-up, that **specific tasks and functions related to the processing of personal data be performed by persons expressly appointed to do so, operating under his/her authority**.

This is done in order to better guarantee technical and specialised supervision during these operations and an appropriate internal distribution of tasks and functions.

The Data Controller Representative is therefore the natural person appointed by the Data Controller and authorised by the latter to perform the activities aimed at guaranteeing constant and strict compliance with the laws in force concerning personal data processing, as well as to represent the Data Controller in dealings with data subjects and the Authorities and in all deeds and contracts of appointment of third parties. This mandate, conferred with a special power of attorney, must be adequately publicised, also internally.

3.5 Data Processor (Group Companies and Third Parties)

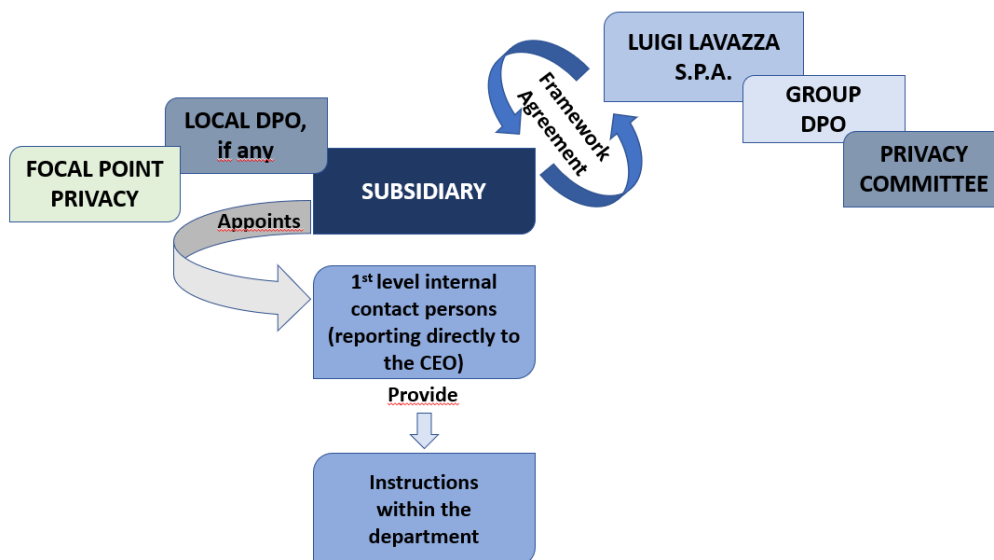
The Data Processor is the natural or legal person that processes personal data on behalf of the Data Controller.

Personal data may be processed in the name and on behalf of the Data Controller by companies appointed by the latter to do so (Group member companies or Third Parties), subject to the signing of a specific contract.

3.5.1 Group member companies

Within the framework of the Group organisation defined in the P.O.M. (see paragraph 3.2 above), the subsidiaries, whether located in or our outside the EU/EEA, in their capacity as **Data Processor**, sign ad hoc agreements on the processing of personal data (the so-called “**Framework Agreements**” or “**Data Processing Agreements**”), aimed at regulating - within the context of **intra-group relations** - the nature, purpose and duration of the processing, types of personal data, the categories of data subjects, and the obligations and rights of the Data Controller.

Organisation of Lavazza Subsidiaries (Data processors)



3.5.2 Third Parties

When it is carried out by Third Parties, i.e., **service providers, business partners or consultants that - in their capacity as natural or legal persons - process personal data on behalf of the Data Controller or the Data Processor company**, the processing is regulated by an agreement or other legal deed that binds the Third Party to the company and regulates, as a minimum, the nature, purpose and duration of the processing; the type of personal data and data subject categories; the prohibition on the transfer of personal data outside the EU; the implementation of adequate security measures and procedures; and the obligations and rights of the Data Controller.

These parties, expressly identified as "**Data Processors**" with a specific deed/contract of appointment (the so-called "**Data Processing Agreement**" or "**DPA**"), must provide sufficient guarantees in terms of the specialist knowledge, reliability and resources necessary to implement adequate technical and organisational measures, also from a security standpoint, so as to guarantee that the processing will protect the rights of the Data Subjects.

The Data Processor, in its turn, can seek help from another data processor (the **Sub-Processor**) **subject to the authorisation of the Data Controller**.

In any event, the Sub-Processor thus appointed by the Data Processor is required to comply with the obligations provided for in the agreement entered into between the Data Controller and the Data Processor.

3.6 Data Protection Officer

In its capacity as Parent Company and "lead" company, LUIGI LAVAZZA S.p.A. has appointed a Group Data Protection Officer (DPO) for all the subsidiaries, for the best coordination at Group level of compliance with the requirements, as well as for monitoring and verifying the application of the provisions of the European Regulation and the company policies and procedures adopted on the subject of privacy.

Taking into account the obligations laid down by local regulations and the specific activities carried out, **local DPOs** can be appointed, who must in any case act in close coordination with the DPO identified at Group level and can make use of the support of the Privacy Committee set up within the Parent Company.

Possible specific requirements or regulatory obligations will, on a case-by-case basis, prompt the appointment of local DPOs.

In general, the Group DPO has the following tasks:

- promptly inform and provide advice to the Subsidiaries - Data Controllers or Processors - on the processing of personal data, availing himself/herself of the support of the Corporate Affairs & Compliance department of the parent company LUIGI LAVAZZA S.p.A.;
- support all the Group company departments in dealing with the issues that have an impact on the processing of this data;
- monitor compliance with applicable regulatory requirements;
- organise the compilation and updating of the Registers of Processing Activities (see paragraph 4) for the Group member companies, monitor the processing with the support of the Internal Contact Persons and the Authorised Processors.

These tasks are carried out by the DPO in **full autonomy and independence**, guaranteed by the fact that the **DPO reports directly to the Board of Directors of the Parent Company**, to whom the DPO is required to send **periodic reports** on the main activities carried out.

The accountability required of Group member companies in the regulation and control of privacy issues, as well as the risk-based approach, entail the need to adopt risk assessments and adequate technical and organisational measures from the conception and design phase of each processing operation (the so-called "**Privacy by design**" principle, see paragraph 8). Each company department called upon to set up a new

activity that may involve the processing of personal data, or the use of new methods in pre-existing processing operations, **must contact the Group DPO, and, where applicable, the local DPO, beforehand for all the detailed information and the checks on compliance**, risk assessment and security issues.

3.7 Privacy Committee

The Privacy Committee, established within the Parent Company LUIGI LAVAZZA S.p.A., is responsible for coordination the application of the privacy regulation; it is composed of representatives of the relevant HQ departments (HR, Internal Audit, Legal and Corporate Affairs, ICT, Digital Marketing, Marketing Italy and others identified on a case-by-case basis) with the task of providing support to the Parent Company and its Subsidiaries in evaluating personal data processing operations that may have significant impacts on company activities.

3.8 Privacy Focal Point of the LAVAZZA Group member companies

In order to facilitate the interaction between the (local and Group) DPOs and the Group member companies, a **"Privacy Focal Point" (PFP)** has been identified within each subsidiary for the management of all the local issues and specific features concerning the processing of personal data.

The Privacy Focal Point is identified by the General Manager/Regional Director of each subsidiary, with the following tasks:

- promptly update local and Group DPOs on problems with the processing of personal data that may arise at the subsidiary where the FP operates, such as, for example:
 - a possible Data Breach;
 - destruction, or loss, whether accidental or deliberate, of personal data;
 - unauthorised access to personal data;
 - new projects or processing modalities affecting privacy;
 - problems in the management of the rights of Data Subjects;
 - new Third Parties involved in the processing of personal data;
- support the company's Internal Contact Persons in risk assessment activities;
- regularly maintain and update the Register of Processing Activities in collaboration with the DPO and the Internal Contact Persons.

3.9 Internal Contact Persons of the LAVAZZA Group member companies

The Internal Contact Persons are the people responsible for a company's organisational structures and are **key figures in the processing of personal data**.

More specifically, the LAVAZZA Group has identified the following persons as Internal Contact Persons:

- the managers who report directly to the CEO, limited to LUIGI LAVAZZA S.p.A. (**first-level "Internal Contact Persons"**);
- the managers that report directly to the Controller (General Manager/Regional Director), with reference to the Group member companies (**first-level "Internal Contact Persons"**);
- the managers of the individual departments, identified and appointed by the first-level Internal Contact Persons, who within the companies of the Group process personal data and/or special personal data categories (**second-level "Internal Contact Persons"**).

Each Internal Contact Person, according to their qualifications and hierarchical and functional powers appropriate to the nature of the responsibilities entrusted to them, has the task of ensuring and overseeing the implementation of technical, organisational and system measures, as well as to supervise, also on the basis of the general instructions imparted by the Controller, or by the General Manager/Regional Director, the performance of the processing operations carried out by the Authorised Processors within the organisational structure the Internal Contact Person is responsible for.

The main tasks of the Internal Contact Person are:

- collaborate with the Data Controller, or with the General Manager/Regional Director, in the fulfilment of the obligations laid down by privacy regulations;
- implement the principles of "Privacy by Design" and "Privacy by Default" (see paragraph 8) according to the provisions of the Privacy Organisational Model, promptly involving the DPO, also via the Focal Point, in the event of new processing activities or new methods for pre-existing processing activities;
- within the context of his/her own department, identify the persons authorised to process personal data (the "Authorised Processors"), and draw up and provide specific written instructions on data processing in their areas of activity;
- supervise the processing operations performed by the Authorised Processors in their departments, making sure that the data is processed in compliance with the instructions provided;
- monitor the implementation of the internal processes envisaged to identify (new and pre-existing) processing methods, and verify compliance with the personal data retention periods defined by the Data Controller, making sure, where applicable, that data erasure and/or anonymisation take place in compliance with the instructions given;
- in connection with the processing of data within their departments, supply and regularly update the Register of Processing Activities with the collaboration of the DPO team;
- promptly contact/involve the Group DPO and, if appointed, the local DPO, and the Privacy Focal Point in the event of any requests and/or complaints from third parties regarding the protection of personal data;
- support the Group's DPO/the local DPO and the Data Controller with the detection and management of potential personal data breaches, ensuring the necessary collaboration in conducting recovery activities (investigation, mitigation and elimination of the consequences of the breach) and updating the Data Breach Register.

3.10 Authorised Processors

The Authorised Processors, namely the persons authorised to perform personal data processing operations, operate on the basis of special written instructions given by their Internal Contact Person for the processing of data in the Authorised Processor's area of activity.

Authorised Processors must limit themselves to processing personal data to the extent strictly necessary for **the performance of their duties and in compliance with the operating instructions received**, under the direct authority of the Data Controller.

For a responsible management that complies with existing laws and regulations, the Authorised Processors who collect, use and store personal data must perform the following tasks in their areas of activity:

- keep personal data accurate and up to date, from its collection to its destruction;
- protect personal data so that it is not accessible to an indefinite number of people or in any event to unauthorised parties or parties that do not have a valid business reason for accessing the information;
- prevent the unlawful or improper use of personal data, if its use is not compatible with the purposes for which it was initially collected;
- ensure that personal data can be tracked and traced (access, alterations, storage) throughout its entire life-cycle;
- retain personal data only for the time required for the purpose indicated and/or for the time provided for by the applicable laws and/or regulations, and, in any case, in compliance with the instructions given;
- promptly report any Privacy breach (unauthorised access to the systems, loss, theft, destruction or erasure of data) to the IT Service Desk, as well as to the local "Focal Point", to their Internal Contact Persons and - in the most serious cases - to the Group and local DPOs;

- do not store personal data in files unprotected by passwords and/or in external hard disks or laptops, the theft or loss of which could result in a Data Breach;

and collaborate with the DPO and their Internal Contact Persons on the compilation and regular updating of the Register of Processing Activities.

3.10.1 CCTV Footage Authorised Processors

The CCTV Footage Authorised Processor is the person responsible for corporate Security that is authorised by the Data Controller/the Data Processor or by the Internal Contact Person of a Subsidiary to **process the images, whether recorded or not, that are captured by the video surveillance systems installed at the offices of the Company for purposes of the protection of company property.**

If, within the framework of a security services agreement with the Company, a third party is authorised to perform such processing operations on the images collected by the video surveillance system on behalf of the LAVAZZA Group, this party must be appointed as "Data Processor".

The Companies in the LAVAZZA Group process personal data using video surveillance systems installed at their offices and plants, and hence are required to comply with regulatory requirements on video surveillance⁹.

4. Register of Processing Activities

Pursuant to the provisions set out in the GDPR, each Group member company that processes personal data is required to maintain a **Register of Processing Activities**, for the activities carried out under its responsibility. The Register, to consist of written records, possibly in electronic format, must be available to the competent authorities.

The Parent Company, LUIGI LAVAZZA S.p.A., has adopted a single Group tool dedicated to the maintenance of the Register of the processing activities carried out by each Group member company, in which the individual processing operations performed by the company departments and functions, the requests from the data subjects, impact assessments, the data processors, the relative DPAs, and the like are recorded.

The Register of Processing Activities is **an integral part of a proper personal data management system and the Privacy Organizational Model**; it is compiled and updated periodically for each Group member company.

5. Management Model

The processing of personal data must be carried out **lawfully, correctly and transparently**, limited to the extent necessary to achieve the purposes indicated in the privacy policy and, in any case, compatibly with such purposes.

There are three phases in the life-cycle of personal data:

- Collection;
- Processing;
- Termination of the Processing and Erasure.

⁹ Provision of the Italian Data Protection Authority on video surveillance of 8 April 2010 and "Guidelines 3/2019 on processing of personal data through video devices" of the European Data Protection Board (EDPB) .

5.1 Collection

5.1.1 Purposes

The processing of personal data (collected or received) by the LAVAZZA Group companies must be performed for **the pursuit of legitimate purposes**.

The personal data collected must be **adequate, relevant and limited** to the extent necessary for the purposes of its processing.

Some of these purposes are listed below, by way of exemplification:

- management of relationships with customers and suppliers (natural persons);
- personnel selection and hiring and management of the employment relationships;
- sending out advertising material and other promotional and marketing initiatives;
- direct sales activities;
- analysis of consumer habits and choices and statistical analysis;
- profiling;
- management of access to the offices of Group Companies and video surveillance.

5.1.2 Legal Basis

For each data processing operation, it is necessary to identify the **legal basis justifying the processing**, i.e., the reasons legitimising the processing of personal data.

For the personal data processed within the LAVAZZA Group, the **legal bases** of the processing are:

- **the consent of the data subject**: when the data processing is explicitly authorised by the data subject for one or more specific purposes (e.g., using the data subject's data for marketing purposes)
- **the performance of a contract or pre-contractual clauses**: when the processing is necessary for the performance a contract in the interest of the data subject (e.g., to dispatch items purchased by a customer, the personal data of that customer, such as name, surname, address, etc., must be collected)
- **the fulfilment of a legal obligation**: when data processing is required by a law, regulation, etc. (e.g., to bill a customer for the purchase of goods, it is necessary to collect their tax data, etc.)
- **a legitimate interest of the Controller**: when the processing is necessary to meet specific needs of the data controller, provided that the processing is not excessively invasive for the data subject (e.g., installing a video surveillance system for security purposes).

5.1.2.1 Consent

Consent, where required as a **pre-condition for the lawfulness of the processing**, must be given via an affirmative act by which the Data Subject manifests his/her **free, specific, informed and unambiguous intention** to accept the processing of his/her personal data, **either in writing** (including by electronic means, e.g., by ticking a box on a website) or **verbally**.

Silence, pre-ticked boxes or inactivity does not constitute consent.

Consent is to be regarded as **freely given** if the Data Subject has a genuine and free choice and is able to refuse or withdraw consent without detriment.

It is presumed that consent is not given freely if:

- the performance of an agreement or the provision of a service are subject to the provision of consent, despite such consent not being necessary for the performance of the agreement.
- it is not possible to give a separate consent to different personal data processing operations.

Explicit **consent**, in fact, must be requested **for each specific purpose of the processing** in an intelligible and easily accessible form. When the processing has **several purposes**, consent should be given for each of them¹⁰.

The burden of proof as to explicit consent having been given lies with the Data Controller (and/or the Data Processor), which must be able to demonstrate that the Data Subject has expressly given his/her consent to the data processing.

If the consent is given **verbally** (e.g., via telephone in the course of marketing activities entrusted to a call centre), the operators appointed to contact lists of names and to manage telephone conversations aimed at promotional activities and/or the collection of information, are expressly required to use specially prepared scripts for the Privacy Notice and the collection of consent, and must record, transcribe and document in writing the consents given.

The consent of the Data Subjects **is not necessary** for the performance of several processing steps, i.e., for:

- the performance of an agreement to which the Data Subject is a party or the performance of pre-contractual measures adopted at the request of the latter;
- the fulfilment of a legal obligation to which the Data Controller is subject;
- the pursuit of a legitimate interest of the Data Controller, as long as such interest is not overridden by the interests or the fundamental rights and freedoms of the Data Subject.

Several examples of the purposes requiring the collection of specific consent are given below:

- sending out advertising material and other promotional and marketing initiatives;
- profiling¹¹, i.e., data processing designed to analyse consumer preferences, habits and choices;
- activities concerning the processing of special data categories, i.e., the so-called **special data** (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data, data concerning a person's health or sex life or sexual orientation), as well as the processing of **personal data concerning criminal convictions and offences**, where required by law.

Data Subjects can **withdraw** a consent previously given at any time to the performance of certain processing operations.

In this case, the processing operations carried out by virtue of said consent must be **promptly interrupted**, unless there is a legal basis for the processing (such as, for example, the fulfilment of a legal obligation; the defence of a legal claim; conditions of legitimate interest of the Data Controller that override the interests, rights and fundamental freedoms of the Data Subject).

In all cases, consent and withdrawals must be appropriately traced, so as to be able to document any amendments/changes requested by the Data Subjects.

¹⁰ If the processing for a purpose other than that for which the personal data was collected is not based on the consent of the Data Subject, the processing for the additional and different purpose must be **compatible** with the purposes for which the personal data was initially collected (taking into account the connection between the purposes, the context in which the data was collected, the nature of the data, the possible consequences of further processing and the existence of adequate guarantees).

¹¹ **Profiling** is a form of automated processing of personal data carried out to evaluate personal aspects relating to a natural person, and, in particular, to analyse or predict aspects concerning the data subject's performance at work, his/her economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where this has legal effects on him/her or affects the person to a similarly significantly extent.

5.1.2.2 Contract performance

Performance of a contract may be used as a legal basis for data processing when the processing is **necessary** to the performance of a contract to which the data subject is a party or the performance of pre-contractual measures adopted at the request of the latter.

Since **necessity** is a fundamental **criterion** for this legal basis, data processing will be legitimate only when the contract cannot be fully performed without the processing of personal data (e.g., for a contract to be signed, it is necessary to request the identification data of the data subject concerned). Accordingly, this legal basis cannot be used when the personal data is not necessary for signing a contract (e.g., for marketing purposes).

For data processing using this legal basis to be deemed legitimate, it will be necessary to **prove**:

- the existence of a contract between the company and the data subject;
- the validity of the contract in question;
- that the processing of the data provided by the data subject is objectively necessary for the performance of the contract.

A privacy notice specifying the legal basis of the processing must always be supplied.

5.1.2.3 Fulfilment of a legal obligation

This legal basis finds application when the processing of personal data is necessary to the **fulfilment of legal obligations**.

This applies to the processing of personal data for the management of administrative and tax requirements to be met by companies within the framework of employment relationships (e.g., payslip management, etc.).

However, the legal obligation must satisfy four conditions:

- It must be **defined by a law**, either an EU law or a national law of a member country;
- The legal provisions in question must establish a **binding obligation to process personal data** that is sufficiently clear and precise;
- Such provisions must at least define the purposes of the processing;
- The obligation must be imposed on the data controller and not on the data subjects.

In such cases, the consent of the data subject is not required, but a privacy notice indicating the legal basis of the processing should still be provided.

5.1.2.4 Legitimate interest

When the processing of personal data is necessary to pursue a **legitimate interest** of the Data Controller, as long as such interest is not overridden by the interests or the fundamental rights and freedoms of the data subject, the personal data may be processed without the data subject's prior consent.

To use this legal basis, however, the interests of the Data Controller must be balanced against the rights attributed to the data subject by the applicable regulations on the processing of personal data in order to assess and prove the prevalence of the interests of the Data Controller over the rights of the data subject.

When carrying out the **balancing of interests** (the so-called "Legitimate Interest Assessment" or "LIA") it is necessary to assess:

- whether **the processing is really necessary**, taking into account the **possible harm** that would be caused to the Controller if it did not carry out the processing;
- the **impact** on the data subjects and their **reasonable expectation** as to what is going to happen to their personal data;
- the **presence of additional data protection measures** that may limit the impact of the processing on the data subjects.

Group member companies are required to conduct such balancing of interests whenever the processing of personal data is based on the criterion of legitimate interest, with the support of the Group's and/or the local DPO, if appointed.

5.1.3 Privacy Notice

Pursuant to the principles of **correctness and transparency** of the data processing, the data subject must be informed of the existence of the processing and its purposes.

The Data Controller must give the data subject full information on the processing of his/her personal data, in a **concise, understandable and easily accessible form** in a clear and intelligible language, in writing or by other means, including in electronic format (website).

The modalities by which personal data is collected, used, accessed or otherwise processed must be **transparent** to the data subjects. In particular, the specific purposes of the processing must be **explicit** and **legitimate** and must be specified at the time when the data is collected.

The Privacy Notice¹² must be given to the data subject **at the time the personal data is collected** or, if the data is obtained from another source, **within a reasonable time period**, at the latest **within one month**. If the personal data is to be used to communicate with the Data Subject or with another recipient, the Privacy Notice is to be provided no later than the first time the data is communicated.

In the case of data collected directly from the data subject, the latter must be informed of any obligation to provide personal data and of the consequences of his/her refusal to do so.

In the event of new processing operations or new methods of carrying out pre-existing processing operations, each company department shall contact the DPO in advance, also through the Privacy Focal Point, for in-depth analyses and checks on compliance aspects (regulations, risk and security analysis).

5.2 Processing – General Principles

The processing operations carried out by the LAVAZZA Group member companies must comply with the general principles laid down by the law and stated below:

- **Lawfulness, correctness and transparency:** the data must be processed lawfully, correctly and transparently in relation to the Data Subject;

¹² The LAVAZZA Group informs all data subjects on:

- type of personal data processed;
- the purpose for which personal data is collected and the legal basis for processing;
- the nature of the provision of personal data;
- data processing methods;
- data communication and transfer methods;
- retention periods;
- the processing of data of minors;
- the rights of the Data Subjects and how to exercise them.

- **Purpose limitation:** the data must be collected for specified, explicit and legitimate purposes, specifically declared and written in a clear and intelligible form in the privacy notice, not further processed in a manner that is incompatible with those purposes. Using the data collected for any purposes other than those stated in the privacy notice is not permitted: if the Data Controller intends to process the personal data further for a purpose other than that for which it was initially collected, prior to this further processing the Data Controller must provide the Data Subject with a new Privacy Notice and, if necessary, new express consent must be given by the Data Subject;
- **Minimisation of data:** the data must be adequate, relevant and limited to the extent necessary for the purposes of its processing;
- **Accuracy:** the data must be accurate and, where necessary, kept up-to-date. All reasonable measures must be adopted to promptly rectify or erase inaccurate personal data;
- **Limitation of data retention:** the data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed to be attained;
- **Integrity and confidentiality:** the data must be processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against loss, destruction, alteration, unauthorised disclosure or access that may cause damage, using appropriate technical and organisational measures.

5.2.1 Processing carried out by Third Parties

Personal data processed by Third Parties means all the cases where the data belonging to LAVAZZA Group member companies, or for which Group companies have been appointed as Data Processors, is made accessible in any way, also via remote connection, to Third Parties.

The provisions of paragraph 3.5 are applicable to these cases.

5.2.2 Cross-border transfer of personal data – intra-group flows

The cross-border transfer of personal data to countries outside the EU/EEA may increase the risk of the data subject being unable to exercise his/her data protection rights, in particular, the right to protect him / herself from the unlawful use or disclosure of that information.

When personal data is transferred from the EU/EEA to Data Controllers or Data Processors in third countries (outside the EU/EEA), the level of protection of natural persons ensured in the EU by the European Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or other third countries.

The transfer of personal data to a third country (to be understood as all cases where the data is accessible in a foreign country, also via simple remote access) may only be carried out to pursue the purpose communicated to the data subject at the time of collection of the data and in compliance with the specific provisions on the transfer of personal data abroad.

Personal data which is undergoing processing or is intended for processing after transfer to a third country may only be transferred to countries that - based on a decision of the European Commission - guarantee an appropriate level of protection (transfer on the basis of an **adequacy decision**).

In the absence of an adequacy decision, and without prejudice to the cases where the transfer is permitted by law (including explicit consent of the data subject; the transfer is necessary for the performance of contractual/pre-contractual measures; the transfer is necessary to exercise or defend a legal claim), the Data Controller must compensate for the lack of protection arising from the transfer of the personal data to third countries with **appropriate safeguards** to protect the data subjects, including the availability of enforceable data subject rights and effective legal remedies, alternatively through:

- **Binding Corporate Rules (BCRs)**, approved by a supervisory authority, aimed at allowing the transfer of personal data from the territory of the State to third countries between companies that are part of the same group of undertakings. These are implemented in a document containing a series of clauses (*rules*) that set out the binding principles that all the companies belonging to the same (*corporate*) group are required to respect^{13 14};
- **Standard Contract Clauses (SCCs)** adopted by the Commission or adopted by a supervisory authority and approved by the Commission;
- **(Ad hoc) Model Contract Clauses** authorised by a supervisory authority;
- **Codes of conduct** are rules of conduct or standard practices drawn up by various international bodies or even by individual States, intended to contribute to the correct application of the Regulation, as a function of sector-specific circumstances and the specific needs of micro, small and medium-sized enterprises;
- **Certification mechanisms** are forms of accreditation that make it possible to obtain from a third party (certification body (CB)) a certificate attesting compliance of the processing carried out with the General Data Protection Regulation (GDPR).

5.2.3 Cookies and similar technologies

The websites of LVAZZA Group member companies may use cookies or similar technologies for **profiling and marketing** activities, in particular in order to analyse or be able to predict aspects concerning a data subject's preferences, habits or consumer choices or personal interests and provide targeted services or advertising contents, show contents and propose business initiatives.

With the exception of those necessary for the websites to work properly, cookies can be used subject to the data subject's prior consent. Consent is acquired by opening a banner visible to users when they visit the website for the first time, where data subjects are invited to express their preferences with regard to the use of cookies (the so-called **cookie manager**).

¹³ BCRs are a mechanism for alleviating the burdens placed on multinational companies in connection with intra-group personal data flows. The issue of an authorisation (by the Italian Data Protection Authority) for the transfer of personal data (from Italy to third countries) through Binding Corporate Rules, in fact, enables multinational group member companies, even if established in different countries, that have thus requested, to transfer personal data within their group of enterprises without the need for further formalities, provided that the provisions laid down in the text of the BCR are observed and the data is transferred for the sole purposes stated therein.

¹⁴ Multinational groups using the BCRs have several responsibilities, including: the preparation of a training programme for their employees on the protection of personal data; the implementation of a system to manage disputes and reports relating to the BCRs; the regular performance of audits for the purposes of verifying compliance with the BCRs by Group member companies; the creation of a team for monitoring compliance with the BCRs and managing reports from Data Subjects.

Besides enabling users to give or refuse their consent to various categories of cookies, the cookie manager also enables them to obtain granular information on the various cookie categories or on each individual cookie, such as the purposes of a cookie, its duration and category (technical, analytical, marketing, profiling).

Consent, where given, is acquired lawfully (on the requirements for consent to be valid, see section 5.1.3 dedicated to this matter) and is traced in order to document the choice of the data subject.

5.2.4 Security

Within the context of the processing operations carried out, the Group member companies adopt measures to ensure a **level of security appropriate to the risks that are presented by processing**.

In particular, personal data must be processed in a manner that ensures **appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against loss, destruction, alteration, or unauthorised disclosure or access, using appropriate technical and organisational measures.

Taking into account the state-of-the-art, the costs of implementation with regard to the risks posed and the nature of the personal data to be protected, the measures to be implemented include:

- stringent checks on physical access;
- restrictions to only authorised personnel for specific sensitive areas (Human Resources archive, Control Room, video surveillance systems)
- secure destruction of paper documents containing personal data;
- secure erasure of IT supports used to process sensitive data that are intended for some other use;
- pseudonymisation or encoding of personal data;
- prompt recovery of availability of, and access to, personal data in the event of a physical or technical accident;
- implementation of protective measures for the networks, systems and software used to process personal data;
- application of the Privacy by Design and Privacy by Default principles (see paragraph 8) in system design and the design of company processes and procedures;
- processes, tools and organisation to ensure the prompt reporting of any unauthorised attempts to access personal data;
- data breach management procedures;
- adoption of solutions to trace the activities carried out on personal data;
- adequate operating practices to regularly test, check and assess the effectiveness of the technical and organisational measures put in place for ensuring the security of the processing.

5.3 Specific processing: Termination of the processing - Erasure and Destruction

The Group member companies subject to the application of this Policy are required to:

- take every reasonable step to **promptly erase or rectify** data that is inaccurate, having regard to the purposes for which it is processed;
- ensure that the **period for which the personal data is retained is limited to a strict minimum**, having regard to the specific purposes for its collection and processing.

In order to ensure that personal data is not stored for any longer than necessary, a **deadline should be established for the termination of the processing and for erasure**.

The data retention period, as well as the criteria used to define this period in relation to the various processing activities recorded in the Register of Processing Activities, is defined in the dedicated Guideline - *Data Retention by processing Groups*.

When a Group member company no longer wants to perform one or several processing operations, the personal data (in paper and electronic format) previously used in connection with such operations - without prejudice to the retention period stated above and the fulfilment of the legal obligations or the purposes to do with the exercise or the defence of a legal claim - must be **erased**.

In particular, the LAVAZZA Group guarantees that the IT supports – e.g., computers (PCs or laptops) or mobile phones – assigned to other employees are properly formatted, and that, when such devices are disposed of at end-of-life, appropriate erasure or destruction procedures are implemented to prevent the disclosure, whether accidental or deliberate, of personal data.

6. Rights of the data subject and handling of requests

A data subject has the right to access to personal data that has been collected concerning him or her, and to exercise that right easily in order to be aware of, and verify, the lawfulness of the processing.

In particular, all Data Subjects have the right to know and obtain communication in particular with regard to:

- the purposes and the time period for which their personal data is processed;
- the recipients of their personal data;
- the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing.

The Group member companies facilitate and cannot refuse to satisfy a data subject's request to exercise his/her rights, unless they can prove that they are unable to identify the data subject.

The Data Subject must be provided with the information requested **without undue delay** and in any event, at the latest, **within one month** of receipt of the request, subject to extension - in cases permitted by law - on account the complexity and the number of requests.


Below are the rights of Data Subjects laid down by the regulation on personal data protection.

6.1 Right of Access

The data subject has the right to obtain from the Controller confirmation as to whether or not personal data concerning him or her is being processed, and, if so, have access to the personal data and receive a copy of the data undergoing processing.

6.2 Right to rectification

The Data Subject has the right to obtain the rectification of inaccurate personal data concerning him/her without undue delay, as well as the right to have incomplete personal data completed, including by means of providing a supplementary statement.

A decorative graphic in the top left corner consisting of a yellow circle, a grey textured circle, and a yellow line.

6.3 Right to erasure

The Data Subject has the right to obtain the erasure of personal data concerning him/her and the Data Controller is required to erase personal data without undue delay, where one of the following grounds applies:

- the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- the Data Subject withdraws the consent on which the processing is based and there is no other legal ground for the processing (such as, for example, the fulfilment of a legal obligation; defending a legal claim; a legitimate interest of the Data Controller that overrides the interests, rights and fundamental freedoms of the Data Subject);
- the Data Subject objects to the processing of the personal data concerning him or her;
- the personal data has been unlawfully processed.

6.4 Right to restriction of processing

The Data Subject has the right to obtain the restriction of processing when, *inter alia*:

- he/she contests the accuracy of the personal data, for the time it takes the Data Controller to verify the accuracy of the data in question;
- in a case of unlawful processing, the Data Subject opposes the erasure of the personal data and requests the restriction of its use instead;

The methods for restricting the processing of personal data may consist of temporarily transferring the selected data to another processing system, or making the selected data inaccessible to users or temporarily removing published data from a website.

6.5 Right to portability of the data

The Data Subject has the right to receive the personal data concerning him or her, and that he/she has provided, in a structured, commonly used and machine-readable format, as well as the right to send it to another Data Controller without hindrance, if:

- the processing is based on consent or is necessary for the performance of a contract to which the Data Subject is a party; and
- the processing is carried out by automated means.

In exercising his or her right to data portability, the Data Subject has the right to have the personal data transmitted directly from one Controller to another, where technically feasible.

If a certain set of personal data concerns more than one data subject, the right to portability of the data must not adversely affect the rights and freedoms of the other data subjects.

6.6 Right to object

The Data Subject has the right to object at any time to the processing of personal data concerning him or her.

When this right is exercised, no further processing is carried out the personal data unless it can be demonstrated that there are compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the Data Subject, or processing is necessary for the establishment, exercise or defence of a legal claim.

If the personal data is processed for direct marketing purposes, the Data Subject has the right to object - at any time and free of charge – to such processing, including the profiling connected to direct marketing purposes.

6.7 Handling requests and time limits for responding

Prior to responding to a data subject's request to exercise his/her rights, it is essential that the Group member companies take all reasonable measures aimed at verifying the identity of the Data Subject, or the party that is making the request on behalf of the latter, in particular in the context of online services or online identifiers, requesting - if necessary - a copy of a valid identification document.

If the request is made by a person acting on behalf of the data subject, the following must be checked:

- the power of attorney signed by the Data Subject:
- the identity of the Data Subject or that of his or her proxy.

If the request concerns the access to the data of a deceased person, the requesting party must be identified and the necessary steps must be taken to make sure that this person is an heir, or in any case, a person that can legitimately exercise this right.

The response provided to the Data Subject or to his/her proxy should be traceable.

If a request is addressed directly to Customer Service or to the Contact Centre, it will be the task of Customer Service to verify the entire life cycle of the data processed (collection, use, storage, erasure), process the request and confirm the outcome thereof to the data subject.

If any doubts arise as to the interpretation of any requests received, in strict compliance with the response times provided for by law, the Customer Service Manager should involve the DPO and the Privacy Committee in order to agree upon and define the proper action to take.

Only in the case of requests addressed directly by Data Subjects to the DPO through the dedicated channel (email address: privacyDPO@LAVAZZA.com) it will be up to the latter to engage the Customer Service for the necessary verifications and authorise the appropriate actions, giving direct confirmation thereof to the Data Subjects.

7. Operating instructions

In order to deal with any requests from Data Subjects, and especially from customers and/or consumers, with regard to the rights described in paragraph 6, every company in the Lavazza Group notifies to the Data Subjects, via the websites of the Group member companies, the email address of the Group's DPO (privacyDPO@lavazza.com) and that of the local DPO (if appointed) for the activities managed by the Consumer Service.

8. Privacy by design & by default

The principle of accountability of the Data Controller means that the latter must be able to demonstrate compliance with the European Regulation by implementing - from the conception and design phase of the personal data processing activities ("**Privacy by Design**") - appropriate technical and organisational measures and internal policies for ensuring that, by default ("**Privacy by Default**"), only the personal data necessary (in terms of quantity, extent of processing, retention period and accessibility) for each specific purpose of the processing is processed.

These measures, *inter alia*, consist of reducing the processing of personal data to a minimum, pseudonymising the personal data as soon as possible, enabling Data Subjects to verify the processing of

their data, creating and improving security features, and clearly defining the division of internal responsibilities.

With the ultimate purpose of implementing effective solutions for the design of personal data processing methods, information processes and systems that are capable of protecting the data during all stages of its "life-cycle", the LAVAZZA Group puts in place technical and organisational measures to guarantee on a preventive basis the protection of the data processed, by ensuring compliance with the following principles:

- responsibility for the processing of personal data by all Group employees and business partners, in order to safeguard the confidentiality, integrity and availability of the personal data processed;
- providing information to Data Subjects on the methods used by LAVAZZA to collect, use, store and communicate personal data;
- use and retention of data exclusively for the purposes communicated to the Data Subjects and expressly authorised by the latter through explicit consent;
- transferring data to business partners only for the purposes identified in the privacy notice and with an appropriate level of security;
- access to the data restricted to personnel authorised and trained in the management of personal data;
- monitoring the correct application, internally and externally, of the principles and the indications provided in this Policy.

The *Privacy by Design* and *by Default* approaches must consider the entire "life-cycle" of the personal data, from its collection to its erasure, taking all the data processing operations into due consideration (recording, storage, consultation, use, communication and transfer) and safeguarding its confidentiality, integrity and availability, in all the processes/systems/applications used to process the personal data.

These principles must be integrated into the entire organisation of the Group: **when called upon to set up a new activity that may involve the processing of personal data or the use of new methods to carry out pre-existing processing operations, each company department shall contact the DPO beforehand for detailed information and checks on compliance requirements (regulations, risk analysis and security).**

The IT tool used by the LAVAZZA Group to map the processing of data makes it possible to assess potential risks arising from the design of new processing operations and, if necessary, to perform a data protection impact assessment (DPIA) in order to make the due corrections (see paragraph 9).

9. Data Protection Impact Assessment (DPIA)

Where a type of processing, in particular a type using new technologies or applied for the first time, is likely to pose a **high risk** to the rights and freedoms of Data Subjects, **prior to proceeding with the processing**, the Group member companies carry out **an assessment of the impact of the processing operations envisaged on the protection of personal data**, aimed in particular at determining the probability and the severity of the risk, by taking into account the nature, scope, context and purposes of the processing.

The outcome of the assessment should be taken into account when determining the appropriate measures to be adopted and the safeguards to be provided in order to reduce the risk and comply with the provisions of the Regulation.

If such measures cannot be adopted, on account of the available technology or the implementation costs, the supervisory authority must be consulted prior to the launch of the processing activities.

With the assistance of the DPO and the support of the Internal Contact Persons, the impact assessment must be updated on a regular basis and whenever necessary in view of the time elapsed from the initial processing

or when significant changes in type of data processed, processing methods or technological solutions used may have altered the initial analysis to a significant extent.

The assessment takes into consideration the entire "life cycle" of the personal data, from collection to erasure, and takes into account any specific elements required by the particular context in which the processing is carried out (e.g., direct marketing, profiling, data of minors, etc.), as well as the applicable law.

The impact assessment is, in any event, mandatory in the following cases:

- automated processing, including profiling, used to make decisions that may have legal (or similarly significant) effects on the Data Subjects;
- the processing, on a large scale¹⁵, of special categories of personal data that present a high risk to the rights and freedoms of the Data Subjects;
- systematic monitoring of a publicly accessible area on a large scale.

10. Data Transfer Impact Assessment (TIA)

When the personal data processed have to be transferred to Group member companies or Third Parties in Countries outside the EU/EEA that do not ensure an adequate level of protection or a level equivalent to that provided by the GDPR, prior to starting the processing, it is necessary to perform an impact assessment on the transfer of the personal data (Transfer Impact Assessment" or "TIA") aimed at evaluating the regulations in force in the country of destination, and assessing the risks presented, and the severity of such risks, to the rights and freedoms of the data subjects, account duly taken of the nature, scope, context and purposes of the processing.

Group member companies subject to the preparation of the TIA are required to document the transfer impact assessment process and, if requested, make it available to the competent supervisory authority.

The outcome of the assessment must be taken into account when determining the **further measures** to be adopted and the safeguards to be provided in order to reduce the risk and comply with the provisions of the Regulation.

11. Notification in the event of a personal data breach

A Personal Data Breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to data subjects, such as: loss of control over their personal data or limitation of their rights; discrimination, identity theft or fraud; financial loss; damage to reputation; loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

Therefore, in all cases of personal data breach, a LAVAZZA Group company that has suffered the breach must:

- make sure that all the appropriate technological and organisational protection measures as a function of the breach have been implemented;
- promptly inform, and in any case within 24 hours, the Data Controller, the Data Controller Representative (if appointed), and the local DPO and the Group DPO so that the competent

¹⁵ Large-scale processing operations aim to process a considerable amount of personal data that could affect a large number of Data Subjects and could pose a high risk to the rights and freedoms of Data Subjects.

supervisory authority can be notified of the event without undue delay and, where possible, within 72 hours of becoming aware of the breach.

The Lavazza Group, with the support of the DPO, has defined and issued a Data Breach Procedure for the proper management of security incidents concerning personal data. Reference is to be made to this procedure for the operating methods to be applied.

Personal data breaches may include, but are not limited to:

- **irreplaceable loss of data (in either paper or electronic format)** where it has been established that the data cannot possibly be recovered. For example: loss/theft of IT supports, or fires/flooding of paper archives;
- **unauthorised access to data (IT systems or paper archives)** meaning a confidentiality breach of the data contained in these systems or in these archives. For example: a hacking attack conducted by exploiting the vulnerability of the systems or through the illegal use of authentication credentials; the consultation of paper archives, the access to which has been defined as strictly for authorised personnel only;
- **loss of the integrity of data** meaning the irremediable impairment of the correctness, suitability and consistency of data. For example: impairment resulting from the unauthorised alteration of data, human error, information system accidents;
- **communication or dissemination of data (either in electronic or in paper format) to non-legitimised third parties**, including unidentified third parties, e.g., through email or verbally.

As soon as they become known, all personal data breaches must be promptly reported by the person that has become aware thereof:

- for LUIGI LAVAZZA S.p.A., to the Internal Contact Person, the DPO, the IT Governance & Security Manager within the ICT department and the Centralised Service Desk, as well as to the Corporate Affairs & Compliance Department;
- for all subsidiaries, to their Privacy Focal Point, their Internal Contact Person and the Centralised Service Desk; it is the responsibility of the Focal Point and the Internal Contact Person to inform the local DPO, the Group DPO and the IT Governance & Security Manager within HQ's ICT department as well as to the HQ Corporate Affairs & Compliance Department, promptly and within 24 hours at the latest.


Once the report has been received, the DPO will immediately inform the Data Controller and, with the support of the Privacy Committee, will assess the alleged breach.

Only if the event is actually deemed to be a Data Breach, the Data Controller will take stock of the necessary corrective measures (Data Breach mitigation activities) and, unless the breach is unlikely to pose a risk to the rights and freedoms of the Data Subjects, it will inform the competent supervisory authority of the ascertained infringement, **without undue delay** and, where feasible, **within 72 hours of becoming aware of it**.

If the breach poses a **high risk** to the Data Subjects, the Data Controller will send a direct notification to each of the Data Subjects, describing the nature of the breach, without undue delay.

12. Inspections by the Data Protection Authority

The competent supervisory authorities may carry out inspections at the LAVAZZA Group Companies with the aim to verify effective compliance with the legal provisions by the latter.

A decorative graphic in the top left corner consisting of a yellow circle, a coffee bean, and a coffee grinder.

In the course of such inspections, the Group will adopt the precautions and safeguards provided for in the internal regulations on its dealings with public supervisory authorities.

As a rule, the Internal Contact Person and the DPO must be informed at once of any contact with officials from the Data Protection Authority.

Documents or information connected to the processing of personal data can only be handed over to the inspectors with the authorisation of a representative of the Legal Affairs Office of the Parent Company, who must be present during the inspection.

The Group DPO, or the local DPO, if appointed, with the support of the Corporate & Compliance Department of the parent company, LUIGI LAVAZZA S.p.A., will act as the point of contact with the Data Protection Authority for any issues to do with the processing, helping the Authority have access to the information necessary and cooperating with it.

12.1 Rules of conduct during inspections

All personnel in any way involved in the management of inspections by the Supervisory Authority is required to observe the rules of conduct set out by the company where they work, as well as the Policies and procedures regulating to such matters.

Reference is made to the operating methods described in the Inspection Management Procedure (PR_LL_L1).

In general, it is recommended that personnel cooperate with the Supervisory Authority: the duty to cooperate entails the obligation to allow access to documents, in both paper and electronic form, stored in computers and hard discs and any other computer device, the obligation to indicate where the required documents are stored, and the obligation to provide all information requested regardless of the fact that the documents or the information are stored in other places or by parties other than the Group member companies, the Data Controllers or the Data Processors (such as, for example, third-parties acting as data processors).


The answers to any questions asked by the inspectors must refer as much as possible to the procedures adopted and the personal data processing carried out, in such a way as to avoid generic answers, reserving the right – in case of uncertainty – to provide clarifications and/or answers, as well as more detailed documentation, including at a later stage.

13. Training

The training program on privacy issues (courses, recipients, scheduling) is defined, at Group level, on the initiative of the Data Controller, by the HR and the Corporate Affairs & Compliance departments of the Parent Company in coordination with the DPO and the Privacy Committee.

The aim of the program is to train and inform the Internal Contact Persons and the parties authorised to process personal data with regard to:

- legislative frameworks, compliance with laws and the Provisions of the Italian Data Protection Authority;
- types of data and data processing methods;
- privacy management model implemented;
- roles envisaged for the processing of personal data;
- privacy notice and consent, access rights, complaints and penalties;
- the security measures adopted.

A decorative graphic in the top left corner consisting of three coffee beans and a yellow circle, with thin yellow lines extending from the beans.

In the cases of newly-hired staff, changes in duties or the introduction of new significant tools for the processing of personal data, the HR department - with the support of the Privacy Committee - is responsible for ensuring that the training plan is updated and deployed in reasonably short times.

The LAVAZZA Group makes available online training courses, to be delivered via the training portal, to all employees in possession of an IT support (PC or mobile phone), and classroom training course for first-level Internal Contact Persons (managers that report directly to the CEO and GMs).

14. Audits

The Internal Audit Department of the Group, within the scope of the activities provided for in the Audit plan, can carry out assurance activities on the level of compliance with the rules set out in this document and the legal framework of reference, starting with the results of any inspections carried out by the DPO or by specifically appointed parties, reserving the right, if necessary, to obtain more in-depth information and/or conduct further *ad hoc* inspections.

Audit activities may also be extended to Third Parties (suppliers) who operate in the name and on behalf of Group member companies.

15. Penalties

An infringement of the laws on personal data protection may expose the Group member companies to various types of liability and the ensuing penalties (of an administrative and/or of a penal nature) depending on the laws that have been breached and may have a significant negative impact on the reputation of the LAVAZZA Group.

Non-compliance with the obligations set out in this Policy constitutes conduct that is relevant for disciplinary purposes and may result in the application of disciplinary measures as provided for by the laws in force and national labour agreements.