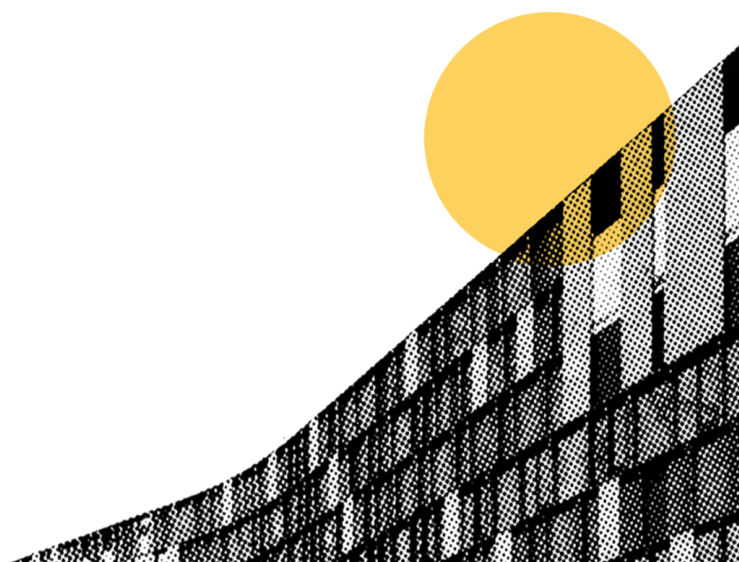




Group Privacy Policy

2020

Version date:
October 2020





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.

Release	Date	Description	
V. 2	October 2020	First release: November 2018	
ISSUING DEPARTMENT:		<i>Policies, Guidelines and Procedures</i>	
PROCESS OWNER:		<i>DPO</i>	
VERIFIED BY:		<i>Legal Affair</i>	
		<i>HR</i>	
		<i>IT</i>	
		<i>Internal Auditing</i>	
APPROVED BY:		<i>CEO</i>	

CONTENTS

1. INTRODUCTION	4
2. GENERAL PRINCIPLES.....	8
2.1 INTRODUCTION	8
2.2 DEFINITION OF PERSONAL DATA	9
3. PRIVACY ORGANISATIONAL MODEL (P.O.M.)	10
3.1 INTRODUCTION	10
3.2 DATA CONTROLLER.....	10
3.3 DATA CONTROLLER REPRESENTATIVE	11
3.4 DATA PROCESSOR (COMPANIES OF THE GROUP AND THIRD PARTIES)	11
3.4.1 Companies of the Group	11
3.4.2 Third Parties	12
3.5 DATA PROTECTION OFFICER	13
3.6 PRIVACY COMMITTEE.....	13
3.7 PRIVACY FOCAL POINT OF THE COMPANIES OF THE GROUP	14
3.8 INTERNAL CONTACT PERSONS OF THE COMPANIES OF THE GROUP	15
3.9 AUTHORISED PROCESSORS	16
3.9.1 Authorised of the Video Surveillance system	16
4. DATA PROCESSING REGISTER	17
5. MANAGEMENT MODEL	17
5.1 COLLECTION	17
5.1.1 Purposes.....	17
5.1.2 Privacy Policy.....	18
5.1.3 Consent	18
5.2 PROCESSING – GENERAL PRINCIPLES.....	19
5.2.1 Processing carried out by Third Parties	20
5.2.2 Transfer of personal data to third countries – intra-group flows	20
5.2.3 Cookies and similar technology.....	21
5.2.4 Security	21
5.3 SPECIFIC PROCESSING: TERMINATION OF THE PROCESSING – ERASURE AND DESTRUCTION.....	22
6. RIGHTS OF THE DATA SUBJECT AND THE HANDLING OF REQUESTS	23
6.1 RIGHT OF ACCESS	23
6.2 RIGHT TO RECTIFICATION	23
6.3 RIGHT TO ERASURE	23
6.4 RIGHT TO RESTRICTION OF PROCESSING	23
6.5 RIGHT TO PORTABILITY OF THE DATA	24
6.6 RIGHT TO OBJECT	24
6.7 HANDLING OF REQUESTS AND ENVISAGED TIME LIMITS.....	24
7. OPERATING INSTRUCTIONS	25
8. PRIVACY BY DESIGN & BY DEFAULT	25
9. DATA PROTECTION IMPACT ASSESSMENT (DPIA)	26
10. NOTIFICATION IN THE EVENT OF A PERSONAL DATA BREACH	27
11. INSPECTION BY THE DATA PROTECTION AUTHORITY.....	28
11.1 RULES OF CONDUCT DURING INSPECTIONS.....	28
12. TRAINING	29



13.	AUDIT	29
14.	PENALTIES	29
15.	ANNEXES	30

1. Introduction

Objective and purpose

This Policy is applicable to LUIGI LAVAZZA S.p.A. and/or its associated companies (hereinafter "LAVAZZA Group") for the processing of personal data (as defined hereafter in paragraph 2.2) during the performance of business activities.

The purpose of this document is the regulation of personal data processing within the LAVAZZA Group, in order 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" indicated below.

This Policy may be implemented and supplemented, where necessary, following instructions from the Policies, Guidelines and Procedures Department of the Parent Company LUIGI LAVAZZA S.p.A.

PRIVACY PRINCIPLELS

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 provide any type of support for the goods and services offered by the companies of the LAVAZZA Group, in relation to which they perform processing operations on personal data, are appointed as **Data Processors** and are contractually obliged to comply with the measures for the security and confidentiality of the data, as well as refraining 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 to contribute to the achievement of this objective.

Communication of personal data

Personal data may be **communicated** to third parties in order to comply with legal obligations, to respect orders issued by public authorities authorised to do so, or to enforce or defend a legal claim, as well as within the context of the companies forming part of the LAVAZZA Group due to business requirements and for 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 subject to appropriate information aimed at specifying the purposes of the processing.

Personal data is not **disclosed**.

Storage

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



Retention Policy, with the exception of the case when there are different storage requirements laid down by local regulations.

Employment relationships

With reference to the data that the company processes in the performance of **employment relationships**, the LAVAZZA Group uses personal data only for the achievement of connected purposes (such as, for example, performance of the employment relationship, 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 with the **consent** of the Data Subjects if required by law, the LAVAZZA Group may process personal data for the achievement of business and marketing purposes (such as, for example: the sending of 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 reasonable precaution to protect personal data** from undue disclosure, alteration or improper use. The protective measures put in place are targeted, in particular, at reducing to a minimum the risk of destruction or loss, including accidental destruction or loss, of the data, as well as any processing that is not permitted or that is non-compliant with the purposes for which it has been collected.

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

Assessment

The LAVAZZA Group performs a **regular self-assessment** in order to check 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 integrate 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).



Glossary

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

- **Authorised Processor:** natural person authorised to physically carry out personal data processing on behalf of the Data Controller. Personnel are authorised to process personal data;
- **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 people authorised to process the personal data under the direct authority of the data controller or the data processor or expressly appointed, in any form, also by being made available, being consulted or combined;
- **Privacy Committee:** group responsible for the coordination of the application of the privacy policy established within the Parent Company and made up of representatives from the relevant HQ departments (HR, Internal Audit, Legal and Corporate Affairs, ICT, Digital, Marketing and others identified on a base-to-base basis);
- **Subsidiary:** all the companies directly or indirectly controlled by Luigi LAVAZZA S.p.A.
- **Identification Data:** the identification data is the data that can be used to obtain the direct identification of the data subject. For example, identification codes, including those derived from personal 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"), 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 data:** Personal Data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or membership to trade unions, and that processes genetic data, biometric data 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 Protection Officer (or "DPO"):** The "Data Protection Officer" is the person designated by the data controller or 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 connected to the processing of personal data;
- **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 deeds and contracts appointing third parties;
- **Disclosure:** the communication of personal data to unspecified parties, in any form, also by making it available or its consultation;
- **Data Protection Impact Assessment ("DPIA"):** assessment of possible risks connected to personal data processing and the impact that the occurrence of the identified risks may have on the rights and freedoms of data subjects;
- **Privacy Focal Point:** natural person appointed within each subsidiary as the point of contact between the subsidiary itself and the Group DPO, responsible for facilitating the management of all the local issues and specific features concerning 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 of the protection of personal data;
- **LAVAZZA Group:** Luigi LAVAZZA S.p.A. and all its Subsidiaries;
- **Headquarters (HQ):** 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 case to whom the data refers;
- **Internal Contact Person:** natural person responsible for supporting the Data Controller with the proper management and verification of the compliance of the processing of Personal Data carried out within his/her Directorate/Department;
- **Data Processor:** the party (natural or legal person) appointed as 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 the assigned responsibilities;
- **Data Controller:** the natural or legal person, public authority, service or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. The data controller also has the task of ensuring the implementation of the technical and organisational measures to ensure a level of security appropriate to the risk presented;
- **Processing:** means any operation or set of operations performed whether or not by automated means, concerning the collection, recording, organisation, storage, consultation, processing, alteration, selection, retrieval, alignment, use, combination, blockage, dissemination, disclosure, erasure or destruction of personal data, even if not recorded in a database;
- **Data breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2. General Principles

2.1 Introduction

European Regulation no. 2016/679¹, better known with the 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 personal data**, aimed at uniformly regulating the rights of European citizens on privacy.

These rules were created in order to **enhance the trust of data subjects**, making them more aware of how their personal data concerning them is used and rendering them free to make an informed decision as to give their consent or otherwise to its use ².

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, the **Code of Ethics of the LAVAZZA Group** states *"the commitment to providing maximum diligence in the collection of personal data and its storage; when processing data, to use the most technically-appropriate tools and to implement all measures and precautions necessary or appropriate to guarantee the security and confidentiality of such data; to not communicate or disclose the personal data that the Group has become aware of in the performance of its business in any way to unauthorised third parties"*.

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

Employees and partners of the LAVAZZA Group, at all levels, are therefore obliged 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 not further processed in a way incompatible with these purposes (*"Principle of purpose limitation"*);

¹ The GDPR was approved by the European Parliament and entered into force on 25 May 2016, but its effects remained suspended until **25 May 2018**, the date when the European Regulation became directly applicable and binding in all the Member States. On 10 August 2018, Italian Legislative Decree no.101 on *"Provisions to adapt national legislation to the provisions of Regulation (EU) 2016/679"* was issued to coordinate with pre-existing Italian legislation.

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, regardless of whether the processing takes place in the Union or not**; (ii) those established outside the EU, but that manage the data of European consumers, offering products and services within the territory of the EU (irrespective of whether there is a connected payment).

- must be **appropriate, pertinent and limited to the extent necessary** for 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 enables identification by 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 the protection - using appropriate technical and organisational measures - against unauthorised or 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** and involves the **assessment, management and ongoing monitoring of risk**.

Each Privacy Contact Person (Internal Contact Person) of the Companies of the Group, as identified in subsequent paragraph 3.7, **has the task of ensuring compliance with this Policy in his/her area of responsibility**.

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

Compliance with the provisions on 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 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 of Business Ethics, also constitutes an **important opportunity for rationalising, classifying and sorting the personal data stored in the company according to updated criteria of necessity and security, limiting the excess duplication of data and avoiding the risks associated with the processing thereof**.

2.2 Definition of personal data³

Personal data means **any information relating to an identified or identifiable natural person ('Data Subject'), 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 factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person⁵

³ The GDPR is not applicable to the processing of personal data in the course 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 is not applicable 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 not or no longer identifiable. The Regulation does not therefore concern 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** 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** (Companies of the Group and Third Parties) and possible Sub-Processors
- **Data Protection Officer**, local and of the Group
- **Privacy Committee**
- **Privacy Focal Point** of the Companies of the Group
- **Internal Contact Persons** (first and second level) of the Companies of the Group
- **Authorised Processors.**

3.2 Data Controller

The Data Controller is the natural or legal person that, alone or jointly with others, determines the purposes and means of the processing of personal data.

On the basis of this definition - taking into account Group assessment activities performed on the type of personal data processed, on intra-group processing, on organisational processes, on technological safeguards and on centralised decision-making processes at HQ level - it is considered that, **generally and subject to exceptions, the Main Establishment⁶, where decisions on the processing of personal data are made, is the registered office of the Parent Company LUIGI LAVAZZA S.p.A. – Via Bologna n. 32 - Turin (Italy).**

In fact, the main decisions on the purposes and the processing methods are made at the registered office whether or not the data is processed at that office⁷.

LUIGI LAVAZZA S.p.A. therefore has taken on the role of the "lead" company and the sole Data Controller for the processing carried out by the companies of the Group, located in EU territory, for which decisions on the purposes and processing methods of personal data are taken, at HQ level⁸.

Companies of the Group that - due to the type of business or internal organisation - have independent decision-making powers regarding the purposes and processing methods of personal data, are an exception to this organisational model centralised within HQ and are considered to all effects and purposes independent Data Controllers (see Annex 1).

The Data Controller, in the person of the legal representative *pro tempore*, is granted the possibility of assigning, under his/her own responsibility, specific tasks and functions connected to the processing of personal data to expressly delegated parties, who operate under his/her authority.

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

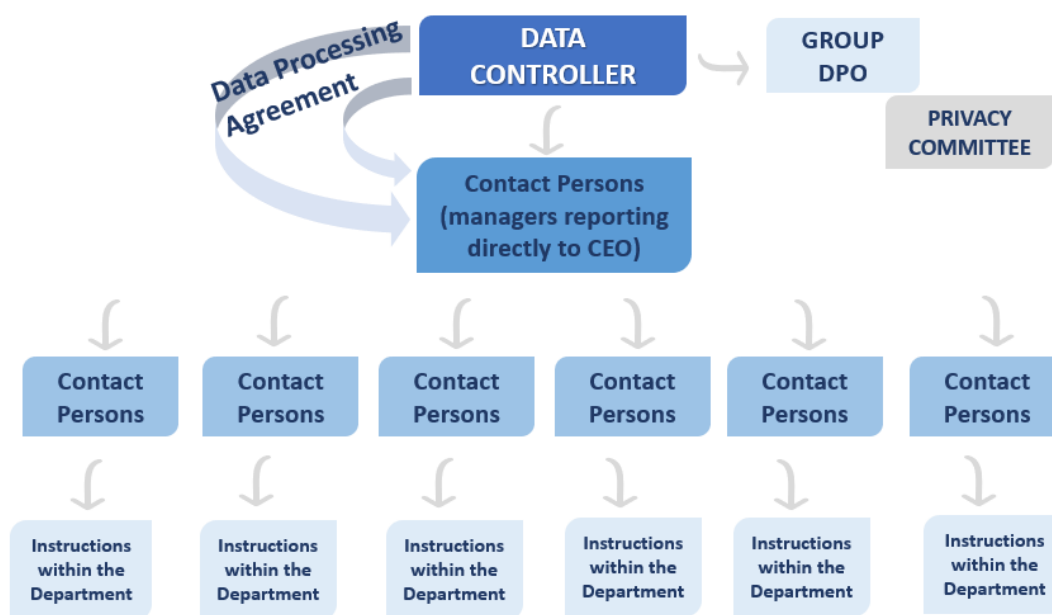
⁷ In compliance, see Recital 36 GDPR.

⁸ In compliance, art.2.1.2 of the Guidelines for the identification of the lead supervisory authority adopted on 5/4/2017 by Article 29 Working Party states that "if processing is carried out by a group of undertakings whose central seat 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, represents the main establishment of the group".

The **proxy**, issued with a special power of attorney by the Chief Executive Officer, must be adequately advertised, also internally.

The Parent Company LUIGI LAVAZZA S.p.A., identifies **first-level "Internal Contact Persons"** from among the managers reporting directly to the CEO, who are responsible for identifying and appointing **second-level "Internal Contact Persons"** within their departments (see paragraph 3.7).

Organisation of Lavazza HQ



3.3 Data Controller Representative

The Data Controller can, under its own responsibility and within the context of its organisational structure, **delegate** specific tasks and functions connected to personal data processing in order to better guarantee technical and specialised supervision during these operations and the proper internal distribution of tasks and functions.

The Data Controller Representative is therefore the 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 data subjects and the Authorities and in all deeds and contracts appointing third parties.

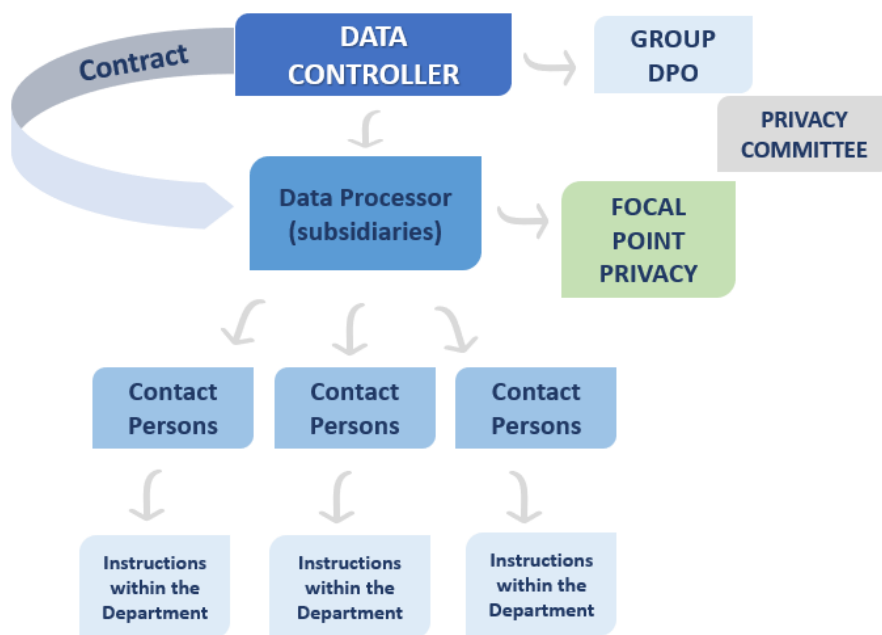
3.4 Data Processor (Companies of the Group and Third Parties)

3.4.1 Companies of the Group

Within the Group organisation (see paragraph 3.2 above), the Parent Company LUIGI LAVAZZA S.p.A., in its capacity as sole Data Controller, has concluded special standard agreements ("**Data Protection Agreements**" -**DPA**) with several subsidiaries, located in Member States of the EU, aimed at regulating - within the context of **intra-group relations** - the nature, purpose and duration of the processing, the type of personal data, categories of data subjects, and the obligations and rights of the Data Controller. In these agreements, the subsidiaries are considered to be **Data Processors**.

Each subsidiary - Data Processor - identifies the **"Internal Contact Persons"** of the subsidiary from among the managers reporting directly to the head of the subsidiary (General Manager) (see paragraph 3.7).

Organisation of Lavazza Subsidiaries (Data processors)



3.4.2 Third Parties

When data is processed by a natural or legal person (Third Parties), **service providers or business partners that process personal data on behalf of the Data Controller**, the processing is regulated by an agreement or other legal deed that binds the Data Processor to the Data Controller and that regulates: the nature, purpose and duration of the processing; the type of personal data and the categories of data subjects; the prohibition on the transfer of personal data outside the EU; the application of adequate security measures and procedures; and the obligations and rights of the Data Controller.

The Privacy Committee (see paragraph 3.5) has the task of defining/updating standard contractual models ("**Data Processing Agreement**") to bind Third Parties to comply with the security measures required by the European Regulation. If the agreements proposed by the Third Parties include clauses that differ from those prepared for the Group, the Privacy Committee and the DPO must be involved for the revision/harmonisation of the aforesaid clauses in order to guarantee compliance with the measures required to protect personal data.

These parties, expressly identified as "**Data Processors**" with a specific deed/contract of appointment, must provide sufficient guarantees in terms of specialist knowledge, reliability and resources to implement adequate technical and organisational measures, also from a security perspective, in order to guarantee that the processing protects the rights of the Data Subjects⁹.

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

In all cases, the Sub-Processor thus appointed, is obliged - **under the responsibility of the Data Processor** - to comply with the same obligations established in the agreement entered into between the Data Controller and the Data Processor.

⁹ The application on the part of the Data Processor of an approved code of conduct or an approved certification mechanism can be used to demonstrate compliance with obligations on the part of the Data Controller.



3.5 Data Protection Officer

The company LUIGI LAVAZZA S.p.A., in its capacity as Parent Company and "lead" company, has appointed a sole Data Protection Officer ("DPO") for all its subsidiary companies for the best coordination at Group level of compliance with obligations, as well as for checking and monitoring of the application of the rules 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 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-to-case basis, prompt the appointment of local DPOs.

In general, the Group DPO has the task of:

- promptly informing and providing advice to the Data Controller on the processing of personal data;
- supporting all the company functions of the Group in the management of the issues having an impact on the processing of this data;
- monitoring compliance with applicable regulatory requirements;

as well as setting up the compilation and updating of the Data Processing Register (see paragraph 4) for the Companies of the Group, monitoring the processing with the support of the Internal Contact Persons and 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**, who are sent **regular reports** on the main activities carried out.

The accountability required of Data Controllers in the regulation and control of privacy issues, as well as the risk-based approach, imply the need to adopt risk assessments and adequate technical and organisational measures from the creation and design phase of each processing operation (so-called principle of "Privacy by design", see para. 8). Each company department - called upon to set up a new activity that may involve the processing of personal data or the management of pre-existing processing with new methods - must contact the DPO beforehand for all detailed information and inspections on compliance requirements (regulations, risk analysis and security).

3.6 Privacy Committee

The Privacy Committee, established within the Parent Company LUIGI LAVAZZA S.p.A., is made up of representatives of the relevant HQ company departments (HR, Internal Audit, Legal and Corporate Affairs and ICT, Digital, Marketing and others identified on a case-to-case basis) with the task of providing specialist support to the Data Controller and to the DPO at regulatory, organisational and process level, as well as with regard to practices on personal data protection.

In general, the Privacy Committee supports the Data Controller and the DPO in the: (i) assessment of compliance of the activities involving the processing of personal data with the requirements of law; and (ii) the preparation of the necessary templates (sample privacy notices, consent forms, appointment and engagement letters, Data Processing Agreements).

3.7 Privacy Focal Point of the Companies of the Group

In order to facilitate the interaction between the (local and Group) DPO and the Companies of the Group - Data Processors, LAVAZZA has identified a **"Focal Point" (FP)** 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 of each subsidiary, with the following tasks:

- promptly updating the DPO on possible problems concerning the processing of personal data, arising within the subsidiary in which the FP operates, such as, for example:
 - possible Data Breach;
 - destruction, or loss, including accidental destruction or loss, of personal data;
 - unauthorised access to personal data;
 - new projects or processing affecting privacy;
 - problems in the management of the rights of Data Subjects;
 - new Third Parties involved in the processing of personal data;
- supporting the Internal Contact Persons of the Company in analysing risk;
- regularly supplying and updating the Data Processing Register in collaboration with the DPO and Internal Contact Persons.

Each Internal Contact Person, according to their qualifications and hierarchical and functional powers appropriate to the nature of the mandate conferred, has the task of guaranteeing and supervising the implementation of the technical, organisational and system measures, as well as to supervise, also on the basis of general instructions given by the Data Controller or the GM, the performance of the processing operations carried out by the Appointed Persons for processing data within the organisational structure they are responsible for.

The main tasks of the Internal Contact Person are as follows:

- to collaborate with the Data Controller and the GM in the fulfilment of the obligations laid down by privacy regulations;
- to 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 or new methods for pre-existing processing;
- to identify, within the context of his/her own department, the persons authorised to process personal data (*"Authorised Processors"*), drawing up and providing specific written instructions for the processing of data in the area of competence;
- to supervise the processing operations performed by the Persons Appointed for processing data in the departments in question, checking that data is processed in compliance with the instructions provided;
- to monitor the application of internal processes adopted to identify (new and pre-existing) processing and to check observance of personal data retention periods defined by the Data Controller, guaranteeing, if envisaged, the erasure and/or making anonymous of the data in compliance with the instructions given;
- with reference to the processing of data within the department in question, to supply and regularly update the Data Processing Register with the collaboration of the DPO and the Privacy Committee;
- to promptly contact/involve the DPO and, where appointed, the Focal Point in the event of any requests and/or complaints from third parties regarding the protection of personal data;
- to support the DPO and the Data Controller in the detection and management of potential personal data breaches, ensuring the necessary collaboration in the recovery activities that may be identified (investigation, mitigation and elimination of the consequences deriving from the breach) and the updating of the Data Breach Register.

3.8 Internal Contact Persons of the companies of the Group

The Internal Contact Persons are parties that, responsible for company organisational structures, are the **key figures in the processing of personal data**.

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

- the managers that 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/GM, with reference to the companies of the Group (**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 categories of special personal data (**second-level "Internal Contact Persons"**).

Each Internal Contact Person, according to their qualifications and hierarchical and functional powers appropriate to the nature of the mandate conferred, has the task of guaranteeing and supervising the implementation of the technical, organisational and system measures, as well as to supervise, also on the basis of general instructions given by the Data Controller or the GM, the performance of the processing operations carried out by the Appointed Persons for processing data within the organisational structure they are responsible for.

The main tasks of the Internal Contact Person are as follows:

- to collaborate with the Data Controller and the GM in the fulfilment of the obligations laid down by privacy regulations;
- to 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 or new methods for pre-existing processing;
- to identify, within the context of his/her own department, the persons authorised to process personal data ("Authorised Processors"), drawing up and providing specific written instructions for the processing of data in the area of competence;
- to supervise the processing operations performed by the Persons Appointed for processing data in the departments in question, checking that data is processed in compliance with the instructions provided;
- to monitor the application of internal processes adopted to identify (new and pre-existing) processing and to check observance of personal data retention periods defined by the Data Controller, guaranteeing, if envisaged, the erasure and/or making anonymous of the data in compliance with the instructions given;
- with reference to the processing of data within the department in question, to supply and regularly update the Data Processing Register with the collaboration of the DPO and the Privacy Committee;
- to promptly contact/involve the DPO and, where appointed, the Focal Point in the event of any requests and/or complaints from third parties regarding the protection of personal data;
- to support the DPO and the Data Controller in the detection and management of potential personal data breaches, ensuring the necessary collaboration in the recovery activities that may be identified (investigation, mitigation and elimination of the consequences deriving from the breach) and the updating of the Data Breach Register.

3.9 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 area of competence.

Each Authorised Processor must limit themselves to processing personal data to the extent strictly necessary in relation to **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 that collect, use and store personal data must ensure the following in their areas of competence:

- to keep the personal data accurate and up to date, from its collection to its destruction;
- to protect the personal so that it is not accessible to an undefined number of people or in any case to unauthorised parties or parties that do not have a valid business reason for accessing the information;
- to prevent the unlawful or improper use of personal data, if its use is not compatible with the purposes for which it has been collected;
- to ensure that personal data can be tracked and recovered (access, alterations, storage) throughout its entire life-cycle;
- to store personal data only for the time required for the purpose indicated and/or for the time laid down by the laws and/or regulations in force, or in any case in compliance with the instructions given;
- to 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 promptly to the local "Focal Point", to his/her Internal Contact Person and - in the most serious cases - to the local and Group DPO;
- to avoid storing personal data on files unprotected by passwords and/or on external hard disks or laptops, the theft or loss of which could result in a Data Breach;

and to collaborate with the DPO and his/her Internal Contact Person in the compilation and regular updating of the Data Processing Register.

3.9.1 Authorised of the Video Surveillance system

The Authorised of the Video Surveillance system is the person responsible for corporate Security that is authorised by the Data Controller or by the Internal Contact Person to **process the images, recorded or otherwise, that are detected by the video surveillance systems installed at the offices of the Company for the 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 the processing operations on the images collected by the video surveillance system on behalf of the LAVAZZA Group, this party must be appointed "Data Processor".

The Companies of the LAVAZZA Group process personal data using video surveillance systems installed at its offices and factories and are, therefore, obliged to adopt the regulatory requirements applicable to video surveillance¹⁰.

¹⁰ Provision of the Italian Data Protection Authority on video surveillance of 8 April 2010.

4. Data Processing Register

In order to demonstrate that the Data Controller (and the Data Processor) complies with the European Regulation, he/she is responsible for ensuring that a **Data Processing Register** is kept. The Register, kept in written form, also in electronic format, must be available to the competent authorities.

The Parent Company LUIGI LAVAZZA S.p.A. has a single Group Register which records the individual processing identified and mapped out for each Company. This can be accessed, per area of responsibility and in separate sections, by the (local and Group) DPO, the Internal Contact Persons, the Privacy Committee and the Privacy Focal Points for possible processing updates in their areas of competence.

The Companies of the Group with independent Data Controllers (see Annex 1) will have their own Data Processing Register, under the responsibility of the *pro tempore* legal representative, which can be accessed by the (local or Group) DPO, the Internal Contact Persons, the Privacy Committee and the Privacy Focal Points for the mapping of processing in their areas of competence.

The Data Processing Register is **an integral part of a proper management system of personal data and of the P.O.M.**

The Register is kept and regularly updated by the Internal Contact Persons, following any changes made in their areas of competence, with the support of the (local or Group) DPO and the Privacy Committee.

5. Management Model

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

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

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

5.1 Collection

5.1.1 Purposes

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

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

Several of these purposes are listed below, by way of example:

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

5.1.2 Privacy Policy

The principles of correct and transparent processing require the Data subject to be informed of the existence of the processing and its purposes.

The Data Controller must provide the Data Subject with all the information on the processing of personal data concerning him or her, in a **concise, intelligible and easily accessible** form, with **clear and plain language**, in writing or via other means, also in electronic format (website).

The methods used to collect, use, consult or process personal data must be **transparent** for the Data Subjects. In particular, the specific purposes of the processing of personal data must be **explained and legitimate** and specified at the time of collection of the data.

The privacy policy¹¹ must be provided to the Data Subject **at the time of collection** of the personal data or, if the data is obtained from another source, within a **reasonable time limit** but, at the latest, **within one month**. In the case where the personal data is intended for communication with the Data Subject or with another recipient, the privacy policy must be provided at the latest at the time of first communication of the data.

In the case of data collected directly from the Data Subject, the latter must be informed of the possible obligation of providing the personal data and the consequences in the event of the refusal to do so.

In the case of new processing or new methods for performing pre-existing processing, it will be the responsibility of each company department to contact the DPO beforehand, also via the Privacy Focal Point, for all detailed information and inspections on compliance requirements (regulatory, risk analysis and security). The Privacy Committee will support the DPO in the preparation/adaptation of the privacy policy models and the collection of consent in light of the purposes of the processing.

5.1.3 Consent

Consent, where necessary as a **condition for the lawfulness of the processing**, must be given by a clear affirmative act establishing a **freely given, specific, informed and unambiguous indication** of the Data Subject's agreement to the processing of personal data relating to him or her, such as by a **written statement** (including by electronic means, e.g. by ticking a box when visiting a website) or an **oral statement**.

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 freely given 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;
- or if it does not allow separate consent to be given to different personal data processing operations.

In fact, it is necessary to request express **consent for each specific purpose of the processing** in an intelligible and easily accessible form. When the processing has **multiple purposes**, consent should be given for all of them¹².

¹¹ The LAVAZZA Group informs all its Data Subjects of:

- the type of personal data processed;
- the purpose(s) for which the personal data has been collected and the legal basis of the processing;
- the nature of the provision;
- the data processing methods;
- the data communication and transfer methods;
- the retention period of the data;
- the processing of data of minors;
- the rights of the Data Subjects and related methods for exercising these rights.

¹² If the processing for a purpose other than that for which the personal data has been collected is not based on the consent of the Data Subject, the processing for the other and different purpose must be **compatible** with the purposes for which the personal data



The Data Controller (and/or the Data Processor) is responsible for the burden of proof of the consent given and must be able to demonstrate that the Data Subject has expressly given his/her consent to the processing of data.

In the event of the **oral** collection of consent (e.g. in the performance of marketing activities via telephone 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, must expressly use the scripts prepared specially (with the support of the Privacy Committee) for the Privacy Notice and the collection of consent, and must record, copy and document the consent given in writing.

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

- the performance of an agreement to which the Data Subject is party or the performance of pre-contractual measures adopted on 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, provided that the interests or rights or fundamental freedoms of the Data Subject are not overriding.

Several examples of the purposes for which it is necessary to collect specific consent are given below:

- the sending of advertising material and other promotional and marketing initiatives;
- profiling¹³, i.e. analysis of consumer habits and choices and statistical processing;
- activities concerning the processing of special categories of data, i.e. so-called **special data** (personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation), as well as the processing of **personal data concerning criminal convictions and offences**.

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

In this case, the processing operations carried out by virtue of this 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 prevail over the interests, rights and fundamental freedoms of the Data Subject).

In all cases, consent and withdrawals must be appropriately traced, so that any amendments/changes requested by the Data Subjects can be documented.

5.2 Processing – General Principles

The processing carried out by the Companies of the LAVAZZA Group 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;
- **Purpose limitation:** the data must be collected for specific, explicit and legitimate purposes, specifically declared and written in a clear and intelligible form in the privacy notice, and

has initially been collected (taking into account the connection between the purposes, the context in which the data has been collected, the nature of the data, the possible consequences of further processing and the existence of appropriate safeguards).

¹³ **Profiling** is any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.

subsequently processed with methods that are compatible with these purposes. The use of the data collected for 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 has initially been 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 stored in a form that enables the identification of the Data Subject for a period of time no longer than that necessary for the achievement of the purposes for which it has been processed;
- **Integrity and confidentiality:** the data must be processed in a way that ensures appropriate security of the personal data, including the protection - using appropriate technical and organisational measures - against unauthorised or unlawful processing and from loss, destruction, alteration, unauthorised disclosure or access that may cause damage.

5.2.1 Processing carried out by Third Parties

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

The provisions of paragraph 3.3 are applicable to these cases.

5.2.2 Transfer of personal data to third countries – intra-group flows

When personal data moves across borders outside the EU it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information.

When personal data is transferred from the EU to Data Controllers or other recipients in third countries (outside the EU), the level of protection of natural persons ensured in the EU by this 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 state, also via simple remote access), may only be carried out for the purpose of pursuing the purpose communicated to the Data Subject at the time of collection of the data and in compliance with the specific provisions concerning the transfer of personal data abroad.

Personal data being processed or intended to be processed following transfer to a third country may only be transferred to countries that - upon the decision of the European Commission - guarantee an appropriate level of protection (transfer on the basis of an **adequacy decision**)¹⁴.

In the absence of an adequacy decision, and without prejudice to the cases where the transfer is permitted by law (including the unambiguous consent of the data subject; the need for the transfer for the performance

¹⁴ The countries are identified by the European Commission. The transfers managed through the "Privacy Shield" certification mechanism in place between the USA and the EU (*Implementing Decision (EU) 2016/1250 of the Commission of 12 July 2016 on the adequacy of the protection offered by the EU-US privacy shield*) also fall within this perimeter.

of contractual/pre-contractual measures; the need for the transfer to exercise or defend a legal claim), the Data Controller must compensate for the lack of protection, connected to 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 of effective legal remedies, alternatively through:

- **binding corporate rules (BCR)**, approved by a supervisory authority, aimed at allowing the transfer of personal data from the territory of the State to third countries among companies forming part of the same group of undertakings. These are implemented in a document containing a series of clauses (*rules*) that fix the binding principles that all the companies belonging to the same (*corporate*) group are obliged to respect^{15 16};
- **Standard Clauses** adopted by the Commission or adopted by a supervisory authority and approved by the Commission;
- **(ad hoc) model set of standard contractual clauses** between the Data Controller in the EU and the Data Controller in the third country, authorised by a supervisory authority.

5.2.3 Cookies and similar technology

The websites of the Companies of the LAVAZZA Group may use cookies or similar technology for **profiling and marketing** activities, in particular in order to analyse or predict aspects concerning the Data Subject's preferences, habits or consumer choices or personal interests and to provide targeted services or advertising content, to show content and to offer business initiatives.

Cookies, with the exception of those necessary for the websites to work properly, can be used subject to the consent given by the data subjects. 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 (so-called **cookie manager**).

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

Consent, where given, is acquired lawfully (for the validity requirements of consent, please 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 Data Controller must implement measures to ensure a **level of security appropriate to the risk presented**.

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

¹⁵ The BCR are a mechanism for simplifying the burdens of multinational companies with reference to 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 companies of the multinational group, even if established in different countries, that have thus requested, to transfer personal data within the group of enterprises without the need for further fulfilments, provided that the provisions laid down in the text of the BCR are respected and the data is transferred for the sole purposes stated therein.

¹⁶ Multinational groups that use BCR have several responsibilities, including: the preparation of a training programme for personnel on the protection of personal data ; the implementation of a system to manage disputes and reports connected to the BCR; the regular performance of audits for the purposes of checking compliance with the BCR by the companies of the Group; the creation of a staff group that is responsible for compliance with the BCR and managing reports from Data Subjects.

Taking into account the state-of-the-art, the cost of implementation with regard to risk and the nature of the personal data to be protected the Data Controller will implement in particular:

- strict physical access checks;
- 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 that, used to process sensitive data, are intended for another use;
- pseudonymisation or encoding of personal data;
- prompt recovery of the availability and access to personal data in the event of a physical or technical accident; implementation of network, systems and software protection systems used to process personal data;
- application of the Privacy by Design and by Default principle (see paragraph 8) in the design of the systems and in the design of company processes and procedures;
- processes, tools and organisation to ensure the prompt reporting of any unlawful attempts to access personal data;
- Data Breach management procedures;
- adoption of solutions to trace the activities carried out on personal data;

as well as adequate operating practices to regularly test, check and assess the effectiveness of the technical and organisational measures in place to ensure secure processing.

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

The Data Controller must:

- take every reasonable step to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is **erased or rectified without delay**;
- ensure that the **period for which the personal data is stored 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, the Data Controller must establish a **deadline for the termination of the processing and for its 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 Data Processing Register, is defined in Annex 2 - Data Retention for processing Groups.

In the case where a Company of the Group intends to end the performance of one or several processing operations, the personal data (in paper and electronic format) previously used within the context of these operations, without prejudice to the retention period stated above and without prejudice to the fulfilments linked to legal obligations or the purposes connected to the exercising or defence of a legal claim, must be **erased**.

The LAVAZZA Group guarantees, in particular, that the IT supports will be appropriately formatted in the case of the assignment of computers (PC or laptop) or mobile phones to other employees, as well as, in the case of the retirement of these devices at the end-of-life, that erasure or destruction procedures will be implemented to prevent the disclosure, including accidental disclosure, of data.

6. Rights of the Data Subject and the Handling of Requests

The Data Subject is entitled to access the personal data concerning him/her and to exercise this right easily, in order to be aware of, and verify, the lawfulness of the processing.

In particular, all Data Subjects have the right to be aware of and obtain communication in relation to:

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

The Data Controller facilitates and cannot refuse to satisfy the request of Data Subjects to exercise their rights, unless the Data Controller demonstrates that it is unable to identify the data subject.

The Data Controller provides the Data Subject with the information being requested **without undue delay** and in any case, at the latest, **within one month** from the receipt of the request, without prejudice to an extension - in the cases permitted by law - taking into account the complexity and the number of requests.

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

6.1 Right of Access

The data subject has the right to obtain from the Data Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and a copy of the data being processed.

6.2 Right to rectification

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

6.3 Right to erasure

The Data Subject has the right to obtain from the Data Controller the erasure of personal data concerning him or her and the Data Controller will be obliged 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 of a legal claim; conditions of legitimate interest of the Data Controller that prevail over 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 from the Data Controller when, *inter alia*:

- the accuracy of the personal data is contested, for a period enabling the Data Controller to verify the accuracy of this data;
- the processing is unlawful and 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 the temporary transfer of the selected data to another processing system, of making the selected data inaccessible to users or temporarily removing the data published by 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 has been provided to the Data Controller in a structured, commonly used and machine-readable format, as well as to send it to another Data Controller without hindrance, if:

- the processing is based on consent or if the processing is necessary for the performance of an agreement to which the Data Subject is 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 Data 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 does not 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.

The Data Controller no longer processes the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or 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 oppose - at any time and free of charge - to this processing, therein including the profiling connected to direct marketing purposes.

6.7 Handling of requests and envisaged time limits


Prior to responding to the exercising of the rights, it is essential that the Data Controller adopts all the reasonable measures aimed at checking 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 and the delegated party.

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 check if 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 the person delegated by him/her should be traceable.

A decorative graphic in the top left corner featuring two coffee beans and a yellow circle.

If requests are addressed directly to Customer Service or to the Contact Centre, it will be the task of Customer Service to check the history of the processed data (collection, use, storage, erasure), implementing the requests of the Data Subjects and confirming the outcome thereof to the latter.

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 correct action to be taken.

Only in the case of requests addressed directly by Data Subjects to the DPO through the dedicated channel (email address: privacyDPO@LAVAZZA.com) will the latter be the party that involves Customer Service for the necessary checks and to authorise the action to be taken, directly giving confirmation thereof to the Data Subjects.

7. Operating instructions

Each Company of the LAVAZZA Group, in order to deal with any requests from Data Subjects, in particular from customers and/or consumers, with regard to the rights stated in paragraph 6, informs Data Subjects, on the websites of the Companies of the Group, of the email of the DPO (privacyDPO@lavazza.com) and of the Contact Centre 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 through the adoption - from the creation and design phase of the personal data processing activities ("**Privacy by Design**") - of adequate technical and organisational measures and internal policies suitable for guaranteeing that only the personal data necessary (i.e. the quantity, extent of processing, retention period and accessibility) for each specific processing purpose is processed, by default ("**Privacy by Default**").

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

With the ultimate purpose of implementing design solutions for personal data processing, information processes and IT systems, capable of protecting the data during all its "life-cycle" phases, the LAVAZZA Group implements technical and organisational measures to preventively ensure the protection of the processed data, ensuring compliance with the following principles:

- responsibility for the processing of data by all the employees of the Group and business partners, in order to safeguard the confidentiality, integrity and availability of the personal data processed;
- information provided 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 declared to Data Subjects and expressly authorised through their express consent;
- transfer of data to business partners only for the purposes identified in the privacy notice and with an appropriate level of security;
- access to data restricted to personnel authorised and trained in the management of personal data;
- monitoring of 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 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: **each company department - called upon to set up a new activity that may involve the processing of personal data or the management of pre-existing processing with new methods - must contact the DPO beforehand for all detailed information and inspections 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 deriving 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 using new technologies or if it is being applied for the first time, is likely to result in a **high risk** to the rights and freedoms of Data Subjects, the Data Controller - **prior to the processing** - carries out **an assessment of the impact of the envisaged processing operations on the protection of personal data**, aimed in particular at determining the probability and the seriousness of this risk, 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 and safeguards to be taken in order to reduce the risk and to comply with the provisions of this Regulation.

If these measures cannot be adopted, in consideration of the available technology or implementation costs, the supervisory authority must be consulted prior to the launch of the processing activities.

The impact assessment must be updated by the Data Controller, with the assistance of the DPO and the support of the Internal Contact Persons, on a regular basis or in any case each time the impact assessment is necessary due to the time elapsed from the initial processing or if there are significant changes in the processing of the type of data processed, in the processing methods or in the technological solutions used that may have considerably altered the initial analysis.

The assessment takes the entire "life cycle" of the personal data into consideration, from its 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 applicable law.

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

- automated processing, including profiling, that produces legal effects or that similarly significantly affects Data Subjects;
- the processing, on a large scale¹⁷, of special categories of personal data that present a high risk for the rights and freedoms of the Data Subjects;
- the systematic monitoring of a publicly accessible area on a large scale.

¹⁷ Large-scale processing operations aim to process a considerable amount of personal data that could affect a large number of Data Subjects and that are likely to result in a high risk for the rights and freedoms of Data Subjects.

10. 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, the Company of the LAVAZZA Group that has suffered the breach must:

- check that all the appropriate technological and organisational protection measures on the basis of the breach have been implemented;
- inform the Data Controller (and also the local and Group DPO for information purposes) promptly and in any case within 24 hours, so that the competent supervisory authority can be notified of the event without undue delay and, where possible, within 72 hours from the time the breach becomes known.

The Data Controller, with the support of the DPO and the Privacy Committee, has defined and issued a Data Breach Procedure (Annex 2) 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.


By way of example but without limitation, possible personal data breaches may consist of:

- **irreplaceable loss of data (in either paper or electronic format)** meaning as such the established impossibility of recovering the data. 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 on these systems or in these archives. For example: a hacking attack through the exploitation of the vulnerability of the systems or 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, IT incidents;
- **communication or disclosure of data (either in electronic or paper format) to illegitimate third parties**, including unidentified third parties, for example through email or verbally.

As soon as 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;
- for all foreign subsidiaries, to the Privacy Focal Point, the Internal Contact Person and the Centralised Service Desk; it will be the responsibility of the Focal Point and the Internal Contact Person to inform the local DPO and Group DPO and the IT Governance & Security Manager within the ICT department of HQ promptly and in any case within 24 hours.

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 fault.

A decorative graphic in the top left corner of the page, featuring a yellow circle and several coffee beans arranged in a cluster.

Only in the case where the event is actually considered to be a Data Breach will the Data Controller implement the necessary corrective means (activities to mitigate the Data Breach) and, if it is unlikely that the breach presents a risk to the rights and freedoms of Data Subjects, it will inform the competent supervisory authority of the established breach, **without undue delay** and, where possible, **within 72 hours from the time the breach becomes known**.

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

11. Inspection by the Data protection Authority

The competent supervisory authorities may carry out inspections at the Companies of the LAVAZZA Group aimed at checking the effective application of legal provisions by the latter.

During the inspections carried out by the Supervisory Authority, the Group will adopt all the precautions and safeguards provided for by internal regulations regarding dealings with Supervisory Authorities.

In general, the Internal Contact Person and the DPO must be informed immediately of any contact with officials from the Data Protection Authority.

Documents or information connected to personal data processing may be handed over to the inspectors only 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 is in charge of acting as the point of contact with the Data Protection Authority for questions connected to the processing, for facilitating the access of the Authority to the information necessary and for cooperating with the latter.

11.1 Rules of conduct during inspections

All personnel, holding any position that may be involved in the management of inspections by the Supervisory Authority, must comply with the rules of conduct indicated by the company in which they work, as well as the Policies and procedures regulating these matters.

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

In general, it is recommended that personnel cooperate with the Supervisory Authority: the duty to cooperate implies the obligation to allow access to documents, in both paper and electronic format stored on computers and hard discs and all other computer devices, 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 information are stored in other places or by parties other than the Data Controller (such as, for example, Data Processors).

The responses 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 general responses, reserving the right – in the event of uncertainty – to provide clarifications and/or responses, as well as more detailed documentation, also at a later stage.

A decorative graphic in the top left corner featuring two coffee beans and two yellow circles of different sizes.

12. Training

The training plan on privacy issues (courses, recipients, times) is defined, at Group level, by the Data Controller and the HR department of the Parent Company in coordination with the DPO and the Privacy Committee.

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

- legislative frameworks, compliance with laws and 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;
- security measures adopted.

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 issued in reasonably short times.

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

13. Audit

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 further *ad hoc* inspections.

The Internal Audit Department is also responsible for compliance checks on the Data Processors appointed by the Data Controller, be they Companies of the Group or Third Parties.

14. Penalties

The infringement of the laws in force on personal data protection may expose the Data Controller to various types of responsibilities and consequent penalties (of an administrative and/or criminal 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 relevant conduct for disciplinary purposes and may result in the application of disciplinary measures as provided for by the laws in force and national labour agreements.

Furthermore, any person that suffers material or non-material damage as a result of an infringement of personal data protection provisions will have the right to receive compensation for the damage suffered.

15. Annexes

ANNEX 1 – Data Retention Policy

ANNEX 2 – Data Breach Procedure.