Privacy

European Regulation 2016/679 (GDPR) and Legislative Decree no. 196 of June 30, 2003, as amended by Legislative Decree no. 101 of August 10, 2018

Data Controller

GASTALDI HOLDING SPA

DATA PROTECTION POLICY

(General rules issued by the Holding Company for the Group's Privacy Compliance.)

Sommario

1. INFORMATION ABOUT THE DOCUMENT 3
1.1. PURPOSE 3
1.2. SCOPE OF APPLICATION 3
1.3. REFERENCES 3
1.4. RESPONSIBILITIES 3
1.5. ARCHIVING 3
1.6. ATTACHMENTS 4
2. DATA PROTECTION POLICY 4
2.1. Premesse e Note Applicative 4
2.2. REFERENCES 5
2.3. DEFINITIONS 5
2.4. RULES FOR THE PROCESSING OF PERSONAL DATA 9
2.4.1. Processing of Personal Data 9
2.4.2. PRIVACY NOTES 11
2.4.3. Consent of the Data Subject 12
2.4.4. RIGHTS OF THE DATA SUBJECT 12
2.4.5. PERSONAL DATA MANAGEMENT 17
2.4.6. PRIVACY ROLES 18
2.4.7. Data Breach 24
2.4.8. RETENTION PERIODS 24
2.4.9. CONTRACTS: GUIDELINES FOR DRAFTING DAT PROCESSING AGREEMENTS 25
2.4.10. COMPLIANCE WITH PRIVACY BY DESIGN AND PRIVACY BY DEFAULT PRINCIPLES 26
2.4.11. Data Protection Impact Assessment 26
2.4.12. Monitoring e Reporting 27
2.4.13. RECORDS OF PROCESSING ACTIVITIES 28
2.5. RISK ASSESSMENT 29
2.6. MONITORING AND CONTROL 29

1. INFORMATION ABOUT THE DOCUMENT

1.1. PURPOSE

The purpose of this document is to define a policy - titled "Data Protection Policy" - aimed at outlining the obligations that **all** employees and collaborators (hereinafter collectively referred to as "**Users**") of Gastaldi Holding S.p.A. and the companies within the GASTALDI GROUP (hereinafter collectively referred to **Gastaldi Holding S.p.A.** as "GASTALDI GROUP" or "Group Companies") must adhere to in order to ensure compliance with the European Regulation 2016/679 (the "Privacy Regulation" or "GDPR") and the current national privacy legislation regarding the processing of personal data.

1.2. SCOPE OF APPLICATION

This document applies to all companies within the GASTALDI GROUP.

1.3. REFERENCES

This policy establishes the inter-company framework for oversight and management of matters governed by the aforementioned European Regulation 2016/679 and other applicable regulations related to the protection of Personal Data.

1.4. RESPONSIBILITIES

The responsibilities for the implementation of this procedure are detailed later in this document. The updating of this procedure is the responsibility of the Privacy Coordination Unit within the GASTALDI GROUP

1.5. ARCHIVING

This procedure is available on the company's INTRANET at the following address: [INTRANET URL]. The original signed hardcopy is kept at the Executive Office's Secretariat of Gastaldi Holding S.p.A.

1.6. ATTACHMENTS

1. Employee and Collaborator Information Template
2. Data Processing Register Template (Controller)
3. Data Processing Register Template (Processor)
4. Procedure for Managing Data Subject Rights Template
5. Data Subject Request Register Template
6. Procedure for Handling Violations Template
7. Data Breach Procedure Template
8. Risk Analysis Template for Data Processing Derived from ENISA
9. Personal Data Processing Agreement Template for Processors
10. Appointment as "Data Processing Officer" Template
11. Privacy Contractual Clauses Template
12. Organizational Chart Template

2. DATA PROTECTION POLICY

2.1. PREMESSE E NOTE APPLICATIVE

As defined in section 1.1 "PURPOSE," this Data Protection Policy aims to outline the obligations that all Users of Gastaldi Holding S.p.A. and the Group Companies (individually and collectively referred to as "Controlled Company/ies") must adhere to in order to ensure compliance with the European Regulation 2016/679 (the "Privacy Regulation" or "GDPR") and the current national privacy legislation regarding the processing of personal data.

As a result, all company policies related to privacy and personal data processing adopted by the Group Companies must conform to the principles and guidelines outlined in this Data Protection Policy. Each Controlled Company is allowed to implement measures, including procedural ones, based on their organizational and business peculiarities, for complete and optimal alignment with the current regulations.

It is worth noting that the Privacy Regulation demands a significantly higher level of diligence, attention, and control over personal data processing methods compared to the previous Privacy Code, introducing sanctions of up to 4% of the annual global turnover for violations.

Therefore, it is of paramount importance to review and understand this Data Protection Policy, and all employees, collaborators, and third parties who handle data on behalf of the Group Companies must adhere to its contents.

Therefore, all Users are informed and required to comply with the requirements of this Data Protection Policy and expressly accept its contents.
The execution of personal data processing in a manner that contradicts the principles and guidelines outlined in this Data Protection Policy and the applicable Privacy Regulations (as

detailed below) may constitute grounds for disciplinary actions and/or may lead, in cases stipulated by law, to civil and criminal proceedings.

This Data Protection Policy is structured into the following sections:

- *Rules for the proper processing of personal data and the correct classification and management of information.*
- *Rules for the proper archiving of company documents and for the appropriate and conscious use of information, systems, and services.*
- *Monitoring and control.*

2.2. REFERENCES

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, hereinafter referred to as the "Privacy Regulation" or "GDPR."
2. Legislative Decree no. 196/2003, as amended by Legislative Decree no. 101 of August 10, 2018, hereinafter referred to as the "Privacy Code," as subsequently modified and supplemented by various measures that have followed since August 2018.
3. Guidelines of the European Data Protection Board and the former "Article 29 Working Party."
4. Decisions of the Italian Data Protection Authority.

2.3. DEFINITIONS

The following definitions are taken from Article 4 of the GDPR, which is the primary source for these definitions:

Personal Data: Any information relating to an identified or identifiable natural person (referred to as the "Data Subject"). A natural person is considered identifiable if they can be directly or indirectly identified, particularly by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity (GDPR Article 4 and Considerations C26, C27, C30).

Personal data can only pertain to a natural person (i.e., an individual) and includes sole proprietorships and freelancers. It does not encompass data related to legal entities (i.e., companies). For example, an individual's corporate email address (e.g., name.surname@groupcompany.it) is considered personal data, while a generic corporate email address (e.g., info@groupcompany.it) is not considered personal data.

Special Categories of Personal Data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as 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 (Article 9 of the GDPR).

Special categories of personal data also include:
Health Data: Personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about their health status.
Genetic Data: Personal data related to the inherited or acquired genetic characteristics of a natural person that provides unique information about their physiology or health, particularly resulting from the analysis of a biological sample from the individual.
Biometric Data: Personal data obtained through specific technical processing related to the physical, physiological, or behavioral characteristics of a natural person that allows or confirms their unique identification, such as facial images or fingerprint data.

When processing these special categories of personal data, the GDPR imposes additional and specific obligations.

Data Subject: Refers to the natural person (including sole proprietors and freelancers) to whom personal data relates.

Privacy Notice: Encompasses all the information as specified in Articles 13 and 14 of the GDPR and communications as per Articles 15 to 22 and Article 34 of the GDPR, related to data processing. This information is presented in a concise, transparent, intelligible, and easily accessible form, using simple and clear language, particularly when providing information specifically to minors, and is conveyed by the Data Controller through appropriate measures. Information is provided in writing or by other means, including, if necessary, electronic means. Upon request from the data subject, information can be provided orally, as long as the identity of the data subject is proven by other means (Article 12 GDPR, Considerations C58-C60, C64).

Processing: Encompasses any operation or set of operations, whether or not by automated means, applied to personal data or sets of personal data. These operations include collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction (Article 4 GDPR).

Profiling: Refers to any form of automated processing of personal data involving the use of such data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning their professional performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements (Article 4 GDPR, Considerations C24, C30, C71-C72).

Consent to Processing: Indicates any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative

action, signify agreement to the processing of personal data relating to them (Article 4 GDPR, Considerations C32, C33).

Data Controller: Refers to the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. When the purposes and means of such processing are determined by Union or Member State law, the data controller or the specific criteria for their nomination may be provided for by Union or Member State law (Article 4 GDPR, Consideration C74). In essence, the data controller is the entity that, either alone or in conjunction with others, determines the purposes and means of processing personal data.

Data Processor: Refers to the natural or legal person, public authority, agency, or other body that processes personal data on behalf of the Data Controller (Article 4 GDPR). The data processor is the entity (either a company or an individual) that processes personal data on behalf of the Data Controller.

The category of Data Processors includes, among others, companies that handle payroll processing, personnel research and training, IT infrastructure providers, and, more generally, anyone who processes personal data of customers, employees, and suppliers (to the extent applicable) of the GASTALDI GROUP on behalf of these companies. This applies in all cases where one of the companies within the GASTALDI GROUP enters into a contract that involves access, collection, or use of data belonging to their customers, employees, or suppliers.

Personal Data Breach: Indicates a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored, or otherwise processed (Article 4 GDPR, Consideration C85).

Data Protection Officer (DPO): As per Article 37 of EU Regulation 2016/679 (GDPR), Chapter 1, b) and c). In consideration of the "Guidelines on Data Protection Officers (DPOs) - WP 243 rev.01," especially Chapter 2) "Appointment of a DPO," paragraphs 2.1 - 2.1.2 - 2.1.3 - 2.1.4 - 2.1.5, the Data Controller, Gastaldi Holding S.p.A., represented by its temporary Legal Representative, in consultation with the Privacy Consultant, believes that the appointment of a DPO is not necessary.

Privacy Coordination: Refers to the structure within the Parent Company that is responsible for coordinating organizational activities related to data protection matters, interfacing with the Privacy Consultant. The objective is to ensure the commitment to privacy principles throughout the Group and reduce the exposure to privacy risks for the entire Group. Privacy coordinators from various Group companies may be invited to participate in the Privacy Coordination.

Privacy Contact(s): These are individuals within each of the individual Controlled Companies who serve as the main point of contact for privacy compliance matters within their respective companies. Their responsibilities are described in the following section 2.4.6.2. The Gastaldi Group companies may, based on their size and/or the complexity of the processing activities, establish additional organizational structures internally and delegate privacy-related activities to other individuals identified within the business functions involved in the processing (the "Functions"), while still preserving the responsibilities of the Privacy Contact.

Authorized Personnel for Processing: Refers to any User who has access to personal data processed by the Gastaldi Group, and whose obligations are outlined in this Data Protection Policy and any related instructions.

System Administrators: These are specific highly skilled individuals authorized for data processing, responsible for the management and maintenance of a computing system or its components, as identified in the supervisory authority's decision of November 27, 2008, as revised in 2009, titled "Measures and measures prescribed to data controllers using electronic tools regarding the functions of system administrators." Their duties are better defined in appointment documents or in the policies and procedures adopted by Gastaldi Group companies regarding the processing of personal data.

Supervisory Authority: In the context of Italy, it refers to the Italian Data Protection Authority, known as the Garante per il trattamento dei dati personali. In general, it denotes the National Authority responsible for monitoring compliance with regulations related to the protection of personal data.

Rights of Data Subjects: Under the privacy regulations in their entirety, all data subjects have certain fundamental rights that must be respected without any exceptions. These rights are outlined in Articles 15 to 22 of the GDPR:

- **Right of Access**: Data subjects have the right to obtain confirmation from the data controller whether or not personal data concerning them is being processed and, if so, to access that personal data.
- **Right to Rectification**: Data subjects have the right to obtain from the data controller the rectification of inaccurate personal data concerning them without undue delay. Considering the purposes of the processing, data subjects also have the right to have incomplete personal data completed, including by providing a supplementary statement.
- **Right to Erasure (Right to Be Forgotten)**: Data subjects have the right to obtain from the data controller the erasure of personal data concerning them without undue delay, and the data controller has the obligation to erase personal data without undue delay.
- **Right to Restriction of Processing**: Data subjects have the right to obtain from the data controller restriction of processing in certain specified circumstances.
- **Right to Data Portability**: Data subjects have the right to receive the personal data concerning them in a structured, commonly used, and machine-readable format and have the right to transmit those data to another data controller without hindrance from the data controller to which the personal data have been provided.

- **Right to Object**: Data subjects have the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them which is based on Article 6(1)(e) or (f), including profiling based on those provisions.
- **Automated Decision-Making and Profiling**: Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.
- **Right to Lodge a Complaint with the Supervisory Authority**: Data subjects have the right to lodge a complaint with the supervisory authority.

Gastaldi Group: Refers to the collective term for all the companies controlled by Gastaldi Holding S.p.A.

Privacy Regulations: Refers to the Privacy Code (Codice Privacy), GDPR, as well as any other regulations related to the protection of personal data that are applicable to the processing of personal data, whether already in force or that will come into force during the term of this Data Protection Policy. This also includes provisions, guidelines, and opinions issued by the Italian Data Protection Authority, the Working Group established under Article 29 of Directive 95/46/EC, the European Data Protection Board established under Article 63 and subsequent articles of the GDPR, and any other competent authorities.

2.4. RULES FOR THE PROCESSING OF PERSONAL DATA

2.4.1. PROCESSING OF PERSONAL DATA

Personal data can only be processed for the purposes specified in the Privacy Notice provided to the data subject. Personal data must be processed as follows:

a) Lawfully, fairly, and transparently.

b) Collected and recorded for specific, explicit, and legitimate purposes, and used in further processing operations compatible with those purposes.

c) Adequate, relevant, and not excessive in relation to the purposes for which they are collected or subsequently processed.

d) Accurate and, if necessary, kept up to date (refer to Section 1, Paragraph 2.4.4).

e) Retained in a form that allows the identification of the data subject for no longer than necessary for the purposes for which they were collected or subsequently processed (refer to Section 1, Paragraph 2.4.7).

f) Processed in a manner that ensures adequate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organizational measures.

2.4.1.1. Classification of Personal Data

Personal data is classified under the GDPR into the following categories:

1. **Personal Data**: This category includes any information related to an identified or identifiable natural person (referred to as the "data subject"). A person is considered identifiable if they can be identified, directly or indirectly, based on identifiers such as their name, identification number, location data, online identifier, or one or more characteristics of their physical, physiological, genetic, mental, economic, cultural, or social identity.
2. **Special Categories of Personal Data**: This category includes personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for uniquely identifying a person, data concerning health, or data concerning a person's sex life or sexual orientation.
3. **Personal Data Related to Criminal Convictions and Offenses**: This category encompasses personal data related to criminal convictions and offenses or related security measures.
4. **Profiling, Geolocation, and Behavioral Data**: This category comprises a set of data that collectively allows for any form of automated processing of personal data. It is used to assess specific personal aspects of an individual, particularly for analyzing or predicting aspects related to their professional performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.
5. **Authentication Data**: This category includes codes, passwords, or PINs intended to provide physical or logical access to systems, applications, or premises. It is presumed that only the data subject has knowledge of these authentication credentials.

2.4.1.2. Rules for Data Processing

The personal data mentioned in the point above can only be processed if and to the extent that at least one of the following conditions is met:

a) The Data Subject has given consent to the processing of their personal data for one or more specific purposes.

b) Processing is necessary for the performance of a contract to which the Data Subject is a party or for the performance of pre-contractual measures taken at the Data Subject's request.

c) Processing is necessary to comply with a legal obligation to which the Data Controller is subject.

d) Processing is necessary to protect the vital interests of the Data Subject or of another natural person.

e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

f) Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the interests or

fundamental rights and freedoms of the Data Subject, particularly if the Data Subject is a child.

Furthermore, in the case of data belonging to special categories of personal data, as Article 9 imposes a general prohibition on processing, exceptions for processing must be specified whenever the data is necessary for processing. These exceptions should be selected appropriately from those mentioned in Article 9 of the GDPR. These exceptions must be specified for each individual processing operation.

Particular attention should be given to the processing of personal data relating to criminal convictions and offenses, which should only occur under the control of the public authority or in specific cases mentioned in Article 2.octies of the Privacy Code.

The GDPR requires that the data subject, whose personal data is being processed, be properly informed about the processing of their personal data through the Privacy Notice and provide their free, specific, informed, and unequivocal consent if the personal data is processed for purposes other than the performance of a contract with the Data Subject.

2.4.2. PRIVACY NOTES

The Data Subject must receive an adequate Privacy Notice regarding the processing of their personal data.

This notice should be made available in accordance with Article 13 of the GDPR when personal data is collected directly from the Data Subject.

Conversely, if personal data is received through third parties, as per Article 14 of the GDPR, the Privacy Notice must be provided:

a) Within a reasonable period from obtaining the personal data, but no later than one month, taking into account the specific circumstances in which the personal data is processed.

b) In cases where the personal data is intended for communication with the Data Subject, at the latest upon the first contact with the Data Subject.

c) In cases where communication to another recipient is envisaged, no later than the first communication of the personal data.

The Privacy Notice must contain information required by law, including:

- Identification of the Data Controller;
- The existence or absence of a DPO;
- The methods and purposes for which the processing is carried out;
- The legal bases connected to the purposes;
- Retention periods;
- Procedures for managing Data Subject rights;
- The right to lodge a complaint with the supervisory authority.

Providing this information is crucial to ensure transparency and to inform Data Subjects about how their personal data is being processed and how they can exercise their rights.

Each company within the Group is responsible for preparing and obtaining approval from the Privacy Consultant for the Privacy Notices to be used, based on the type of data processed and its processing.
The updating of the Privacy Notices is the responsibility of the relevant Privacy Contact, who will consult with the Privacy Consultant to ensure the consistency of the privacy notices adopted by the GASTALDI GROUP companies.

Any modifications to the Privacy Notices adopted by Group companies cannot be made without prior written approval from the Privacy Contact, acting as the representative of the Data Controller, and the Privacy Consultant.

2.4.3. CONSENT OF THE DATA SUBJECT

As a general rule, obtaining consent is a complex process, and it's obligatory to stop processing data based on consent upon request. Therefore, special attention should be paid to collecting consent unless there are other legal bases for processing.

Consent is not used for processing the personal data of employees.

However, for specific processing activities where other legal bases are not possible, consent may be used, keeping in mind:

- The adoption of a decision based solely on automated processing of health data, including profiling, for the provision of contractual services, requires explicit and separate consent from the Data Subject, except for specific cases to be evaluated on a case-by-case basis.
- The consent expressed by the Data Subject must be documented in paper, electronic, or recorded format in computer systems to be able to provide proof and prevent violations of the obligations under the Privacy Regulation.
- Every use of consent should be carefully evaluated and reported.

2.4.4. RIGHTS OF THE DATA SUBJECT

All companies within the Group must provide Data Subjects with a postal address and an email address through which Data Subjects can exercise their rights as outlined in Chapter III of the GDPR.

Continuous monitoring of email inboxes and the receipt of postal mail should be in place to ensure that all communications are promptly forwarded to the Privacy Officer for a timely response to the Data Subject.

Similarly, when a Data Subject's request is directed to a third party that processes personal data on behalf of any of the Companies within the GRUPPO GASTALDI (e.g., a supplier, a contractor), such third parties must immediately notify the relevant Privacy Officer and the Privacy Consultant. They should send an email to the designated address specified by the Company in the data processing agreement or other contractual documentation governing the relationship with the third party. Every contractual relationship should explicitly address the processing of personal data.

In coordination with the Privacy Consultant, the competent Privacy Officer for the request to exercise rights or one of their delegates:

a) Must verify the identity of the Data Subject who has submitted the request by comparing the information in the request with the data already held by the relevant Company.

b) In case of discrepancies or legitimate doubts about the identity of the requester, the Privacy Officer should contact the Data Subject using the available contact information and request the submission of a copy of their identification document.

c) Once the identity of the requester is confirmed, the Privacy Officer should:

i. Coordinate with the relevant Company functions based on the request (IT and/or others) to identify the data subject to the request and ensure that it is processed (e.g., in the case of a deletion request) across all IT systems and documents of the Company and its suppliers and/or third parties.

ii. Provide a written response to the requester within 1 month of receiving the request.

d) If the request is particularly complex:

i. The Privacy Officer should, within 1 month of receiving the request, provide a justification for any extension of the response deadline to the Data Subject.

ii. Within two months of communicating the extension, the Privacy Officer should provide a response to the Data Subject.

No charges can be applied to fulfill Data Subject requests except in cases where:

1. The Data Subject's request is manifestly unfounded or excessive due to its repetitive nature (this assessment should be made by the Privacy Officer), or
2. In the case of the right of access, the Data Subject requests additional copies beyond those provided with the initial request.

The response provided to the Data Subject should not only be "intelligible" but also concise, transparent, easily accessible, and formulated in a simple and clear language.

Reference is made to the following paragraph 2.4.4.5 for the procedures for exercising the right to data portability. All requests to exercise rights must be recorded in a register under the responsibility of the Data Protection Officer.

2.4.4.1. Right of Access by the Data Subject[1]

The Data Subject can request confirmation as to whether or not personal data concerning them is being processed and, if so, obtain:

a) access to personal data;

b) access to the following information:

1. the purposes of the processing;
2. the categories of personal data concerned;
3. the recipients or categories of recipients to whom the personal data has been or will be disclosed, in particular recipients in third countries or international organizations;
4. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
5. the existence of the right to request from the Controller the rectification or erasure of personal data or the restriction of processing of personal data concerning the data subject or to object to such processing;
6. the right to lodge a complaint with a supervisory authority;
7. where the data is not collected from the Data Subject, any available information as to their source;
8. the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.

If personal data is transferred to a third country or to an international organization, the Data Subject has the right to be informed of the existence of adequate safeguards under Article 46 of the GDPR.

The Data Subject must be informed of their rights as established in Articles 13 and 14 of the GDPR.

The individual to whom the personal data relates can also request a copy of the processed data, provided that this does not infringe upon the rights and freedoms of other Data Subjects.

2.4.4.2. Right to Rectification and Integration [2]

The Data Subject has the right to obtain the rectification of inaccurate personal data or the completion of incomplete personal data.

[1] Art. 15 del GDPR.
[2] Art. 16 del GDPR.

2.4.4.3. The right to erasure [3]

The data subject has the right to obtain the erasure of their personal data without undue delay if:

a) the data subject's personal data is no longer necessary for the purposes for which they were collected or otherwise processed;

b) the data subject withdraws the consent on which the processing is based, and there is no other legal ground for the processing;

c) the data subject objects to the processing pursuant to Article 21, paragraph 1 of the GDPR, and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21, paragraph 2 of the GDPR (see paragraph 2.4.4.6);

d) the personal data has been unlawfully processed;

e) the personal data must be erased for compliance with a legal obligation;

f) the personal data has been collected in relation to the offer of information society services as referred to in Article 8 of the GDPR.

There may be circumstances in which the data subject's data must be retained for regulatory purposes. In such cases, in consultation with the Privacy Consultant, the competent Privacy Officer or their delegate will collaborate with the relevant company function (IT and/or others) to ensure that the data remains available exclusively for regulatory purposes within the GASTALDI GROUP companies and is made available exclusively to the relevant authorities, adopting technical measures for this purpose.

2.4.4.4. Right of restriction of processing [4]

The data subject can obtain the restriction of the processing of their personal data where:

a) The data subject contests the accuracy of their personal data; the restriction applies for the time strictly necessary for the relevant GASTALDI GROUP company to verify the accuracy of the data;

b) In the case of unlawful processing, the data subject opposes the erasure of personal data and requests that, instead of erasure, the restriction of their use be imposed;

[3] Art. 17 del GDPR.
[4] Art. 18 del GDPR.

c) If the data controller no longer needs or intends to retain the data but the data is necessary for the data subject for the establishment, exercise, or defense of a legal claim;

d) The data subject has objected to the processing under Article 21, paragraph 1, of the GDPR, pending verification of whether the legitimate grounds of the data controller override those of the data subject.

In the above-mentioned circumstances, the Gastaldi Group company will process the data subject's personal data solely for retention purposes, as defined by the competent Privacy Officer in collaboration with the Privacy Consultant, and with the cooperation of the relevant business function (IT and/or other) in the case of data processing carried out using IT methods.

In addition to retention, the Gastaldi Group company may, on the other hand, process the data subject's data - while the processing is limited - only when:

i. The data subject has provided their consent;
ii. For the establishment, exercise, or defense of a legal claim by the company acting as the data controller;
iii. To protect the rights of a third party (natural or legal person);
iv. For significant reasons of public interest.

The right to restriction involves "tagging" the personal data pending further determinations; therefore, it is advisable for the data controllers to implement suitable measures in their information systems (electronic or otherwise) for this purpose.

2.4.4.5. Right to portability [5]

The data subject may request the data controller company to:

a) Obtain the personal data concerning them, and

b) Request the direct transmission of such data to another data controller

in cases where:

i. The processing is carried out by automated means;
ii. The processing is based on the data subject's consent under Article 6(1)(a) or Article 9(2)(a) of the GDPR, or on the existence of a contract to which the data subject is a party under Article 6(1)(b) of the GDPR; and
iii. The data subject-provided data subject to portability (for example, data that have become subject to processing as a result of activities performed by the data subject, such as using a service or a device, and always processed by automated means - paper

[5] Art. 20 del GDPR (C68).

archives and records, and, in general, any data processed with human intervention, are excluded).

2.4.4.6. Right of objection [6]

The data subject has the right to object at any time to the processing of personal data concerning them if it relates to, among other things:

a) Direct marketing purposes, including profiling to the extent it is related to such direct marketing; b) Historical research or statistical purposes.

In the aforementioned circumstances, the data controller refrains from further processing the personal data unless they demonstrate compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject or for the establishment, exercise, or defense of legal claims.

2.4.4.7. Right not to be subject to decisions solely based on automated processing [7]

The data subject also has the possibility to request not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects concerning them or similarly significantly affects their person, except in cases where:

a) It is necessary for the conclusion or performance of a contract between the data subject and the data controller;

b) It is authorized by national or European Union law to which the data controller is subject;

c) It is based on the explicit consent of the data subject

2.4.5. PERSONAL DATA MANAGEMENT

Personal data cannot be disclosed to third parties, including other companies within the Group different from the respective data controller unless the data subject has been properly informed about the legal basis used to enable the transfer. In such cases, all the entities acting on behalf of the data controller (data processors, for example, but not limited to: payroll managers, HR consultants, management consultants, auditors, as well as cloud service providers, managers of IT platforms in use, etc.) are included. These communications must be specifically highlighted in the information provided to data subjects..

[6] Art. 21 del GDPR (C69, C70)
[7] Art. 22 del GDPR

In particular, for all employees, there must be a specific section indicating that data transfers occur based on the legitimate interests of the Company to other companies within the Group, with specific reference to the parent company.
In general, subject to specific exceptions provided by Privacy Regulations, personal data cannot be transferred outside of the member states of the European Economic Area unless specific agreements have been signed with the receiving entity to ensure an adequate level of data protection for data processed outside the territory of the European Union, as provided by Italian and EU regulations.

2.4.6. PRIVACY ROLES

In accordance with Article 37(2) of the GDPR, the GRUPPO GASTALDI parent company has decided NOT to appoint a Data Protection Officer (DPO) but instead to rely on an external Privacy Consultant, who serves as the contact person for all privacy offices of individual companies, where applicable. The Privacy Consultant of the parent company and the Privacy Contacts of each company share a method of exchanging information to standardize behavior regarding inquiries from data subjects and to determine the most appropriate privacy frameworks to use for specific activities or contracts with third parties.

In particular, to ensure effective oversight of the correct processing of personal data by GRUPPO GASTALDI, at least the following appointments are foreseen:

1. A Privacy Consultant for the GRUPPO GASTALDI parent company.
2. A Privacy Contact for each company within GRUPPO GASTALDI.

This Privacy Contact collaborates with the Privacy Consultant for internal coordination within the individual company. In the event of a data breach, the Privacy Contact actively works to provide the consultant with all necessary support for managing the data breach, acting as a liaison between the consultant and the relevant company/department.

It is also important to note that:

1. The Data Controller is the entire legal entity of the company, even when represented by top-level executives, each with their own organizational responsibilities.
2. Data Processors are external parties (other internal or external companies within or outside the group) with whom an agreement on data processing is formalized in accordance with Article 28 of the GDPR.
3. Each employee or collaborator is an Authorized Person for Processing under Article 29 of the GDPR (this privacy function also includes all executives).

Special attention will be given to identifying specific "Authorized Persons for Processing," such as System Administrators, who are professional figures responsible for the management and maintenance of a processing system or its components. They fall within the categories specified in the provision of the Italian Data Protection Authority dated November 27, 2008

(published in the Official Gazette No. 300 of December 24, 2008), as well as its subsequent amendments and additions, regarding "Measures and precautions prescribed to data controllers for processing carried out by electronic tools concerning the allocation of system administrator functions." It should always be kept in mind that security and control measures must be described, applied, and deemed sufficient by the Data Controller.

All employees and collaborators should promptly and adequately involve the relevant Privacy Representative in all matters related to the protection of personal data. The Privacy Representative should always coordinate with the Privacy Consultant if one is present and, if applicable, with the Group Privacy Consultant.

Subsidiary Companies, based on their size, complexity, and the nature of the processing activities they carry out, may or may not designate a Data Protection Officer (DPO). However, there must always be Privacy Representatives responsible for overseeing the entire Personal Data Protection activity within the company.

2.4.6.1. Duties of the Parent Company Privacy Advisor

The Privacy Consultant, in collaboration with the Privacy Representatives, shall:

a) Prepare modifications and corrections to this Data Protection Policy and other procedures defined by GRUPPO GASTALDI concerning personal data processing, with the aim of maintaining consistency in the policies and procedures related to personal data processing across different companies within GRUPPO GASTALDI.

b) Maintain a list of Privacy Representatives from each subsidiary company within the Group.

c) Supervise, through the Privacy Representatives, GRUPPO GASTALDI 's compliance with Data Protection Regulations.

d) Coordinate and oversee the activities of the Privacy Representatives, including through collaborative discussions.

e) Inform and advise the Privacy Representatives regarding their obligations under Data Protection Regulations.

f) Monitor the training and informational activities for individuals authorized to process personal data concerning their obligations under Data Protection Regulations.

g) Collaborate with the Privacy Representatives in the preparation of privacy notices, consent forms, appointments as data processors, and any other relevant matters related to personal data processing. The Privacy Consultant and the Privacy Representatives should serve as the primary point of contact for each company within the Group concerning issues related to personal data processing.

h) Handle internal reports of Data Protection Regulation violations by individuals operating under the authority of the Data Controller, in collaboration with the Privacy Representative of the specific subsidiary company and the respective HR function if applicable.

i) Periodically verify that the Privacy Representatives correctly maintain:

a. Register of processing activities

b. Register of data subject requests

c. Register of events that may become data breaches.

d. register of data breaches

e. list of data processors of the individual Group companies;

j) Collaborate with the Privacy Representatives, when necessary, in responding to data subject requests and ensure they are promptly processed.

k) Periodically or upon request by the Privacy Representatives, verify the content of privacy notices and consent forms.

l) Verify the correctness of the appointments as "Data Processing Controllers" already in place, always in compliance with the contractual agreements signed.

m) Conduct audits, either directly or through questionnaires, to assess the reliability of newly identified data processing controllers.

n) Maintain a list of the privacy notices in use by each company within the Group.

o) Collaborate, with the support and through the Privacy Representatives, with the relevant corporate functions of the Group Companies to ensure compliance with the principles of privacy by design and by default.

p) Provide recommendations in the context of the data protection impact assessment ("DPIA") as provided for in the following Paragraph 2.4.10, and oversee its completion.

q) Cooperate with the Supervisory Authority and act as the point of contact for the Supervisory Authority on matters related to the processing of personal data and, if necessary, on any other matters, including prior consultation as per Article 36 of the GDPR.

r) Perform other activities within their competence as required by the Data Protection Regulation, including this Data Protection Policy and other internal procedures and policies on personal data processing.

All communications to the relevant Supervisory Authority concerning any Group Companies will be archived at the Group Privacy Consultant's office.

2.4.6.2. Duties of the Subsidiaries' Privacy Contact or Privacy Advisor

The Privacy Representatives must ensure compliance with the provisions of the Privacy Regulations and policies issued by GRUPPO GASTALDI within the respective Group Company that has designated them. The Privacy Representatives will also collaborate with the Privacy Consultant and, in particular, must:

a) Inform and provide guidance to the GRUPPO GASTALDI member companies and Users who process data regarding obligations arising from the GDPR as well as other provisions related to personal data protection;

b) Prepare Privacy Notices, consent forms, appointments of data processors, and any other documentation related to the processing of personal data and ensure that it is correctly integrated into the company's processes and products;

c) Maintain:

i. Record of processing activities,

ii. Record of requests from data subjects,

iii. Record of events that could become data breaches,

iv. Record of data breaches,

v. List of data processors for each Group Company;

d) Maintain a historical archive of versions of Privacy Notices in use and appointments of data processors;

e) Ensure compliance with Privacy Regulations to prevent potential violations and subsequent risks and liabilities for the Group Companies, including promoting awareness and training of personnel involved in data processing and related control activities regarding the importance of compliance with data protection obligations;

f) Prepare, with the assistance of appropriate company functions, a Data Protection Impact Assessment ("DPIA") as described in Section 1, Paragraph 2.4.111, and have its content approved by the Legal Representative of the Company;

g) Collaborate with relevant company functions to ensure compliance with the principles of privacy by design and by default;

h) Coordinate the management of any specific and particular privacy policies of individual companies, providing guidance, in consultation with the Privacy Consultant, on matters related to the processing of personal data;

i) Ensure that reporting obligations regarding data processing methods are met;

j) In case they become aware of or suspect that the behavior of their company's appointees does not comply with their obligations, gather additional information and collaborate with the Privacy Consultant to address the violation with them;

k) Bring significant data protection issues to the attention of the Privacy Consultant and collaborate with them on such matters;

l) Perform other activities within their competence as defined by this Data Protection Policy and other internal procedures and policies on data processing.

To enable the Group Privacy Consultant to carry out control activities, the Privacy Referents will also be responsible for:

a) Sending a report to the Group Privacy Consultant at least semi-annually, by January 15th and July 15th of each calendar year, and in case of emergencies (i.e., in the event of a data breach). The report shall be prepared based on the attached template and shall relate to the methods of processing personal data;

b) Conducting periodic checks, at least semi-annually, in collaboration with the Privacy Consultant, within the company functions they deem appropriate, and requesting copies of documentation to support their audit activities;

c) In collaboration with the Privacy Consultant, taking measures to correct any non-compliance with applicable Privacy Regulations or risks of non-compliance based on information contained in the reports, audit findings, or acquired through other means;

d) Conducting periodic checks on system administrators. In the case of system administrators belonging to other group companies, the check must be conducted by the company to which they belong.

In the event of non-compliance with Privacy Regulations by Group Companies or, in general, in the processing of personal data carried out within one of the companies, the Privacy Consultant and the respective competent Privacy Referents are obliged to activate a verification committee. This committee will conclude with a specific report that should outline the plan of actions taken to make the processing compliant. The report, known as an accountability report for the processing, must be brought to the attention of the respective company's owner and the group.

The Privacy Referent is responsible for matters related to compliance with Privacy Regulations in each Group Company. In the event of violations of Privacy Regulations, you can contact the respective competent Privacy Referent and the Privacy Consultant at the addresses specifically provided.

2.4.6.3. Tasks of the Privacy Team

Each company can define, based on its organizational complexity, the categories of data processed, and the number of data subjects involved, a Privacy Team that includes the local IT Manager.

The local Privacy Team itself can be integrated into its composition, depending on the needs and the privacy structure of the Group Company involved, and, depending on specific cases and circumstances, also by the Head of the relevant business function in relation to the issue to be analyzed.

Some members of the Privacy Team are part of the GRUPPO GASTALDI Privacy Committee, which is coordinated by the Group Privacy Consultant.

The "Privacy Committee" is composed of the Group Privacy Officer, the Privacy Consultant, and the legal representative of the company concerned.

The Group Privacy Committee is responsible for analyzing complex, uncodified cases and evaluating any violations related to the processing of personal data (e.g., data breaches) in accordance with the data breach procedure adopted in line with the Standard Model.Altri ruoli

The Persons Authorized for Processing are all employees and collaborators who have access to personal data processed by GRUPPO GASTALDI and receive detailed instructions on the methods of personal data processing.

System Administrators appointed by the companies are professional figures responsible for managing and maintaining a data processing system or its components, falling within the cases specified in the provision of the Garante dated November 27, 2008 (published in the Official Gazette No. 300 of December 24, 2008) and its subsequent amendments and additions ("Measures and precautions prescribed to data controllers for data processing carried out with electronic tools regarding the attributions of system administrator functions"). Their tasks are explained in a specific instruction, prepared by each company according to its specificities.

Every employee should review the list of Privacy Contacts to identify the main contact person for privacy-related matters.

At the time of hiring or entering into a collaboration contract, every employee or collaborator must receive and expressly accept, in addition to the information that specifies the purposes of processing their personal data, this Data Protection Policy. This policy is designed to inform them of their obligations regarding the processing of personal data on behalf of the companies within the GRUPPO GASTALDI, as well as any additional provisions prepared by individual subsidiary companies.

The signing of the contract implies consent for the processing of personal data related to their organizational role, following the detailed instructions of the direct data controller.

Training activities for users are provided to ensure compliance with the Privacy Regulations and this Data Protection Policy. Specifically, each user will need to complete privacy-related courses that will be made available by the company.

It is the responsibility of every employee to periodically undergo privacy training provided by the Group companies. Violation of this obligation may result in disciplinary measures being taken.

Users, in particular, must promptly and adequately involve the Privacy Officer in all matters related to the protection of personal data.

2.4.7. DATA BREACH

Anyone who identifies a case (even just suspected) of significant events regarding personal data has an obligation to report it to the relevant Privacy Officer as soon as possible, supplementing the communication with as much detail as possible based on the model attached to the company's breach management procedure. It will be the responsibility of the company's Privacy Officer to communicate the event to the Privacy Consultant and activate the privacy committee so that the event can be analyzed in detail and any necessary investigations can be carried out to determine whether notification to the Supervisory Authority is required (within a time limit of 72 hours from the discovery of the potential breach) and, if necessary, to the Data Subject.

The Privacy Officer immediately activates the Privacy Committee and works to complete the collection of information so that the Committee has as much information as possible to assess the severity of the event. The Privacy Committee decides whether communication to the Supervisory Authority is necessary and delegates the preparation of the report to the company's Privacy Office, under the supervision of the Group Privacy Consultant, as required by the Supervisory Authority's communication portal. It will be the responsibility of the Data Controller (the company involved) to countersign the submission of the report and ensure that the process is completed within the timeframes prescribed by current legislation. It will be the responsibility of the Group Privacy Consultant to carry out the necessary checks to ensure that any recovery remediation plans are activated within the specified timeframes.

2.4.8. RETENTION PERIODS

Personal data must be processed for the time strictly necessary to fulfill the specific purpose indicated in the Privacy Notice made available to the data subject to whom the data refers, and as specified in that Privacy Notice.
In relation to each category of personal data, the companies within the GRUPPO GASTALDI evaluate the retention periods, which are indicated in the document "Guidelines on the retention of personal data of company X." When the retention period expires, the data is deleted and/or anonymized in accordance with the procedures specified by the software in use.

It will be the responsibility of the Privacy Officer to prepare an accountability document that includes all the retention periods, and this document should be included in the group's retention summary and harmonized across the various companies. The summary may include anonymization or complete de-identification instead of deletion as retention measures.

2.4.9. CONTRACTS: GUIDELINES FOR DRAFTING DAT PROCESSING AGREEMENTS

Whenever a supplier or an external entity accesses personal data processed by companies within the GRUPPO GASTALDI, it is necessary to verify whether that entity is suitable to process personal data on behalf of the companies, in compliance with the applicable Privacy Regulations. This verification must be carried out through additional checks, if necessary, as determined by the Privacy Officer in collaboration with the Group Privacy Consultant.

The verification methods should be included in the request for proposal presented to the external entity. Compliance can only be assessed if it has been specified in advance before the submission of a formal proposal by the external entity.

The standard data processing agreement must be customized by the delegating business unit and must detail the terms of data processing transferred to the external entity.

If the supplier does not provide sufficient guarantees regarding the protection of personal data, it is not possible to entrust the activity to that supplier. However, if the supplier is unique for technical performance and is strategic for the activities of one of the companies within the GRUPPO GASTALDI, the Privacy Committee can be convened to establish the methods for carrying out the processing, activating all mechanisms for the protection of data subjects, and, if necessary, proceeding with pseudonymization managed directly by the company.

If the supplier or third party is capable of providing sufficient guarantees from a technical and organizational standpoint for the processing of personal data, the responsible function within the company must define the personal data processing agreement (appointment) in accordance with the standard defined within the GRUPPO GASTALDI.

Once the agreement is signed, the Privacy Officer must update the register of processing activities and the list of data processing controllers and notify the appointment to the Group Privacy Consultant. An original copy (if in paper format) or the electronically signed appointment letter must be retained by the Group company and made available upon request by the relevant Privacy Officer and/or the Privacy Consultant.

No contract or assignment involving the processing of personal data on behalf of companies within the GRUPPO GASTALDI can be entered into without the prior written authorization of the relevant Privacy Officer and/or the Privacy Consultant, especially if appointment models different from the standard models approved by the same Privacy Officer are used.

2.4.10. COMPLIANCE WITH PRIVACY BY DESIGN AND PRIVACY BY DEFAULT PRINCIPLES

The Privacy Consultant / Privacy Officer of the individual company, either directly or through the supporting structure, shall monitor the proper processing of personal data, their accuracy, reliability, and updating, both during acquisition and processing, within their own function, and send periodic reports to the Group Privacy Consultant based on the instructions provided in the appointment or upon request, regarding the methods of personal data processing within the Group company that appointed them.

Any new processing of personal data carried out by company offices must be reported to the Privacy Officer, who will assess the involvement of the Privacy Committee or the Group Privacy Consultant for the purposes of privacy by design activities as described below and/or the possible update of the processing activities register.

If an User of one of the Group's companies intends to carry out a new activity, develop a new product or service, or update a product or service involving the processing of personal data, they must adhere to the following principles:

i) Privacy by Design Principle: Any project or product must be developed with consideration for data protection issues from the design phase, particularly with regard to:

a. Purpose of processing;
b. Data minimization;
c. Retention periods;
d. Data erasure;
e. Processing methods;
f. Secure software development.

ii) Privacy by Default Principle: Any project or product must ensure that, by default, only the personal data necessary for each specific purpose of processing is processed (this refers to data quality, processing scope, retention period, and accessibility).

To this end, the data controller must follow what is established in the privacy by design and privacy by default management procedure defined by the company in line with the standard defined by GRUPPO GASTALDI.

It is not possible to develop new products or services, tools, or other technical applications or functionalities - aimed at both customers and employees - that involve the processing of personal data, including their updates, without following the guidelines provided in this paragraph.

2.4.11. DATA PROTECTION IMPACT ASSESSMENT

If the Privacy Officer of the individual company deems it necessary for a processing operation to be carried out only after a specific Data Protection Impact Assessment (DPIA) as per Article 35 of the GDPR, the Privacy Officer will instruct the project manager responsible for the development of the product/service to conduct the DPIA. The DPIA should involve the Privacy Officer of the individual company in accordance with the relevant regulations.

The DPIA, once approved by the Privacy Officer of the company, must be submitted to the Group Privacy Consultant for final approval.

It's essential to remember that the Privacy Consultant will:

i) Evaluate whether the measures taken to minimize risks to the personal data of data subjects are adequate. In this case, the Privacy Consultant will prepare a record of the correct execution of the DPIA, which will be maintained by the Privacy Consultant.

ii) If the Privacy Consultant deems that the processing presents a high risk without adequate risk mitigation measures, they will initiate consultation with the relevant Supervisory Authority under Article 36 of the GDPR.

The cases where a DPIA is necessary include, as examples but not limited to:

- Conducting scoring and behavior analysis, including profiling, especially concerning professional performance, economic situation, health, personal preferences or interests, reliability, behavior, location, or movements.
- Making decisions based on automated processing that has legal effects on the data subject or significantly affects them.
- Systematic monitoring of data subjects.
- Processing, on a large scale, of special categories of personal data as defined in Article 9 of the GDPR and data relating to criminal convictions and offenses as defined in Article 10 of the GDPR.
- More generally, any processing on a large scale determined based on the number of data subjects involved, the volume of data processed, and the duration and geographical extent of the processing.
- Combining or matching data, for example, derived from different processing activities conducted for different purposes or by different data controllers.
- Processing personal data of vulnerable individuals, especially minors.
- The innovative use or application of new technologies, such as systems involving the processing of fingerprints or facial recognition.
- Any other processing that, given the nature, scope, context, and purposes of the processing, presents a high risk to the rights and freedoms of individuals.

A DPIA is required if any of the cases mentioned applies. If there is any doubt about whether a DPIA is necessary, the Data Protection Officer (DPO) should seek the opinion of the Privacy Consultant.

2.4.12. MONITORING E REPORTING

The Group Privacy Consultant, in collaboration with the Privacy Representatives of individual companies, conducts periodic checks on the data processing methods of each Group company, including through the reporting required by this Data Protection Policy. If deemed necessary, other forms of control and/or audit may also be employed.

Following these checks, the Group Privacy Consultant will send an annual report, by February 15th of each calendar year and in case of emergencies (e.g., in the event of a data breach), to

the Legal Representative of each Group Company through the Group Privacy Representative. This report will include, for example, but not limited to:

- Requests or investigations by the relevant Supervisory Authority.
- Any observed non-compliance with personal data protection regulations, along with corrective measures taken, risks, or significant issues related to personal data processing.
- Data Protection Impact Assessments conducted and those recommended by the Group Privacy Consultant.
- New projects and their compliance with privacy by design and by default principles.

For internal control activities, the Group Privacy Consultant may also conduct cross-checks (meaning the Privacy Representative of one company can check the privacy activities carried out by another company within the group).
For each audit, a separate report must be prepared and delivered to the audited company and the Group Privacy Consultant.

The recommendations from the Group Privacy Consultant sent to the Legal Representative of each Group Company following their control activities must be evaluated by the Board of Directors of the respective Group Company. If the Company decides not to comply with these recommendations, the decision must be properly justified and documented in the minutes of the relevant Board of Directors meeting.

2.4.13. RECORDS OF PROCESSING ACTIVITIES[8]

It is necessary to ensure the constant updating of the record of processing activities, which should contain at least the following information:

a) The name and contact details of the Data Controller, and where applicable, the Joint Data Controller, the representative of the Data Controller, and the Privacy Officer;
b) The purposes of the processing;
c) A description of the categories of data subjects and categories of personal data;
d) Categories of recipients to whom personal data have been or will be disclosed, including recipients in third countries or international organizations;
e) Transfers of personal data to a third country or international organization, including the identification of the third country or international organization and documentation of suitable safeguards;
f) The envisaged time limits for erasure of the different categories of data;
g) A general description of the technical and organizational security measures implemented.

The record of processing activities should be kept under the responsibility of the Privacy Officer of each individual company, who should update it whenever there is a change in the information contained therein or when a new product or service involving the processing of personal data is identified. Each update to the Register must be communicated to the Group Privacy Consultant, who will maintain a list of valid versions.

[8] Art. 30 del GDPR.

In this regard, if the individual business units of the Group's companies detect a change in the processing of data within their purview or introduce a new product or service, they must immediately notify the Privacy Officer and, in writing, the Privacy Consultant so that they can carry out the necessary checks.

2.5. RISK ASSESSMENT

Each company within the Group must, based on its own organization, prepare a risk assessment, properly documented, within its data processing/business process/information system. The risk assessment should be presented for analysis to the Privacy Committee and the Group Privacy Consultant through the Privacy Officers, in order to be recorded and to define the residual risk with acceptability characteristics. The residual risk should always be formally accepted by the individual data controller through a specific accountability document. Activities related to the risk arising from IT processing should be carried out by the company that manages all information systems, if applicable.

2.6. MONITORING AND CONTROL

For organizational and productivity reasons, as well as for the protection of the company's assets, the Group companies may have the need to control the use of their IT systems. This activity, carried out in accordance with the legitimate interests of the data controller, should not be considered as employee monitoring and is conducted in compliance with Italian labor laws and data protection regulations.

The reasons why the Group companies might conduct monitoring activities include:

a) Identifying and preventing unauthorized access or communication of information.
b) Ensuring compliance with laws and regulations, including internal policies.
c) Preventing and identifying criminal activities.
d) Monitoring for viruses and other malicious code threats.
e) Ensuring business continuity.
f) Investigating or identifying inappropriate use in case of suspicion.
g) Investigating violations of this or other specific company policies in case of suspicion.
h) Responding to a complaint.
i) Conducting a disciplinary or legal investigation.
j) Assisting in the investigation of alleged misconduct.

Particular attention should be given to IT system management activities. These activities are centralized in a Group company that performs them for all others. These activities should be regulated with a specific agreement on the processing of personal data.

Monitoring is carried out within the limits allowed or required by law and as necessary and justifiable for the purposes of the Group companies.

Information identified during monitoring (including personal information) may be used and retained for the duration of any investigative, disciplinary, regulatory, or criminal proceedings

and may be disclosed to third parties when necessary. Any disciplinary proceedings should follow the procedures outlined in the applicable Collective Bargaining Agreement.