PC COMPONENTS EUROPE SRL

Privacy Policy 2024
Privacy Organization Model of PC Components Europe s.r.l.

The document defines the rules and guidelines for the management of personal data processing by the Company according to the provisions of the EU Regulation No. 2016/679 (GDPR) and the relevant Italian legislation

PC COMPONENTS EUROPE SRL

Version	Date	Description
V1	March 2024	First *version*
APPROVED BY:		Sole Administrator Annie Maples

PC COMPONENTS EUROPE SRL

INDEX

1. Introduction

Purpose	This document governs the personal data processing activities of the company PC Components Europe s.r.l. (PCE for short) in accordance with European Regulation No. 2016/679 (GDPR) and the Privacy Code (Legislative Decree No. 196/2003 and subsequent amendments and additions).
Responsibility	All individuals within the Company who are involved in the processing of personal data must contribute to its protection by applying this Policy and the Principles contained herein. Protecting the **confidentiality** of personal data is both a value of the Company and an extremely important goal contributed by all employees.

PRIVACY PRINCIPLES

Treatment and purpose	PCE processes personal data in **accordance with the law, fairly and transparently,** to achieve the **purposes of its business activities.** These purposes must be **determined, explicit and in accordance with the law.** The Company shall take all reasonable measures to ensure that personal data are **accurate** and **up-to-date**.
Third parties	Third Parties are those parties who have business relationships with the Company and, as a function of those relationships, process personal data on behalf of PCE. These individuals are identified as Data **Processors** and are contractually obligated to take the necessary security measures and ensure the confidentiality of the data; among others, they are obligated to refrain from any use or disclosure that is not authorized by PCE.
Disclosure of personal data	Legitimately acquired personal data may be **disclosed** to third parties for the purposes permitted by law and thus to fulfill legal obligations, execute public orders, act before a judge, execute business, labor or cooperation relations, and manage them from an administrative point of view. Personal data may be disclosed to third parties, as autonomous Data Controllers or Data Processors, with the **consent of** the Data Subjects, if required by law, and in any case after providing the information identifying the purposes of the processing. Personal data are not **disseminated**.
Conservation	Personal data are kept only as **long as necessary** to achieve the purposes for which they were collected, in accordance with the law.
Labor relations	PCE uses personal purchased data of **employees**, only for the management of the employment relationship and then for its execution, for the processing of pay slips, for the management of the relationship in tax and social security, to ensure occupational safety, vocational training, performance evaluation; image and video footage of employees may be used for business purposes with prior consent.
Business and marketing activities	With the **consent of** the Data Subjects where required, **according to the law, with fairness and in a transparent manner** PCE may process personal data for business operations and marketing activities, sending, by way of example, informational and advertising material and sales offers.

Security

PCE uses **effective technological tools and measures** to **protect personal data** in order to prevent it from being improperly disseminated, used for other than permitted purposes, or altered.
The measures appresented must **minimize the risks of** loss, unauthorized access, and unauthorized processing or processing inconsistent with the purposes of the collection.
Risks are made the subject of periodic analysis to assess the **continuing appropriateness of the measures provided**, also because of changes in business organization and developments in technology.
Security measures are **constantly monitored** and **periodically checked**.

PCE on a periodic basis verifies that personal data protection measures are concretely applied by all parties involved.

Definitions The following are definitions of key terms for understanding this Model

- **System Administrator**: a person who manages and ensures the maintenance of the computer system or its components as defined by the General Provision of the Italian Privacy Guarantor of November 27, 2008;
- **Supervisory Authority (or Authority)**: the Authority provided for in Article 51 of the GDPR *"one or more independent public authorities responsible for monitoring the application of this Regulation in order to protect the fundamental rights and freedoms of natural persons with regard to processing and to facilitate the free flow of personal data within the Union."* The Italian supervisory authority takes the name Garante Privacy.
- **Authorized processor**: an individual authorized to materially perform processing operations on personal data on behalf of the Controller. Authorized processor is the employee personnel who, by virtue of and limited to their assigned duties, process personal data.
- **Standard Contractual Clauses-SCC**: standard contractual clauses known by the acronym 'SCC that represent contractual templates developed by the European Commission to be applied to relationships between controllers and data controllers in order to comply with the GDPR.
- **Communication**: bringing to the attention of and transferring personal data to one or more determined persons other than the data subject, the owner's representative in the territory of the state, the person in charge and the persons in charge.
- **Data Processing Agreement ("DPA")**: an agreement for the processing of personal data signed between a Data Controller and a Data Processor and aimed at regulating data, purposes and methods of processing as well as the obligations and responsibilities of the parties;
- **Data Protection Impact Assessment ("DPIA"):** data protection impact assessment is the assessment expected by Article 35 of the GDPR that the data controller carries out in cases where the processing involves in particular the use of new technologies that considering the nature, subject, context and purposes of the processing, may present a high risk to the rights and freedoms of natural persons.

- **Data Protection Officer (DPO) or "Data Protection Officer":** is the person designated by the data controller or processor to perform support and control, advisory, training and information functions with respect to the implementation of the GDPR
- **Identifying data: identifying data** are the data that allow identification of the data subject. A distinction is made between **data that allow direct** identification-such as biographical data (for example: first and last name), images, etc. - and **data that** allow **indirect identification-such** as an identification number (e.g., social security number, IP address, license plate number);
- **Personal data**: **Personal data** are information that identifies or makes identifiable, **directly or indirectly,** a natural person and that can provide information about his or her characteristics, habits, lifestyle, personal relationships, health status, economic situation, etc..;
- **Sensitive/particular data:** this refers to data revealing racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, relating to health or sexual life. The GDPR has also included **genetic data, biometric data** and data relating to **sexual orientation in** the notion;
- **Delegate of the Data Controller:** an individual designated by the Data Controller to the performance of useful activities to ensure compliance with current regulations on the processing of personal data, as well as to represent him/her in relations with **third parties;**
- **Dissemination**: the giving of knowledge of personal data to unspecified individuals, in any form, including by making them available or consulting them;
- **General Data Protection Regulation ("GDPR"):** the "*General Data Protection Regulation,*" i.e., Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, which establishes the European regulatory framework in the area of personal data protection;
- **Data subject**: the natural person identified or identifiable, directly or indirectly, by personal data and otherwise to whom the processed data relates;
- Legitimate **Interest Assesment ("LIA**"): is the balancing of the interests of the Data Controller who is processing personal data on the basis of its legitimate interest and the rights and freedoms of the data subjects whose personal data are being processed;
- **Privacy Organizational Model ("P.O.M."):** is the set of rules, procedures, organizational and technical measures adopted to ensure compliance with data protection and privacy regulations**;**
- **Internal Contact** Person**:** an individual responsible for assisting the Data Controller in the proper management of Personal Data processing**;**
- **Data Processor**: the individual (natural or legal person) designated as the Data Processor in relation to the processing of personal data carried out on behalf of the

Data Controller, as a result of a formal act of appointment that defines the scope of responsibilities assigned;

- **Sub-Processor:** the person (natural or legal person) who carries out the processing activities entrusted to him/her by the Processor;
- **Data controller**: the natural or legal person who determines the purposes and means of the processing of personal data. The controller is also responsible for ensuring the implementation of technical and organizational measures to guarantee a level of security appropriate to the risk;
- Transfer Impact Ass**esment ("TIA"):** impact assessment on the transfer of personal data outside the EU and EEA and for which there are no adequate safeguards for the transfer under Chapter V of the GDPR.
- **Personal data transfers**: any transfer of personal data that is processed or intended to be processed after transfer to a third country located outside the EU/EEA for which an adequacy decision has not been issued, including subsequent transfers of personal data from one third country to another third country;
- **Treatment**:
- is any operation or set of operations, performed with or without the aid of automated processes and applied to personal data or sets of personal data**,** such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, comparison or interconnection, restriction, erasure or destruction;
- **Personal Data Breach ("Data Breach")**: a security breach that accidentally or unlawfully results in the destruction, loss, modification, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.

2. General principles

2.1 Background

European Regulation No. 2016/679[1] known as GDPR ("*General Data Protection Regulation*"), is a European Union regulation on the **protection of natural persons with regard to the processing of personal data**, aimed at uniformly regulating the privacy rights of European citizens.

These rules are intended to **strengthen the confidence of data subjects** by increasing their knowledge about how personal information about them is used and by freeing them to make an informed decision about whether or not to consent to its use.

These rules have a significant impact on data that are normally collected and managed in the course of normal business activities, due to the **increased level of personal data protection** brought about by the Regulations.

In the course of carrying out its business activities, PCE collects personal data and information and assumes the obligation to process them in accordance with the relevant regulations.

In particular, **PCE's Code of Ethics** highlights the Company's special attention to the implementation of the requirements for the protection and safeguarding of personal data.
A commitment to confidentiality in the use, processing, and custody of data must be assumed and guaranteed by all employees and non-employee personnel who, in the course of their activities, process personal data on behalf of PCE.

PCE employees and contractors are therefore required to recognize whether they are collecting, using, processing, storing, or sharing personal data that are subject to protection. They must, therefore, be aware of and aware of the **basic principles governing the processing of personal data**, namely that data:

- must be processed in a manner in accordance with the **law, with fairness and transparency to the** data subject, in accordance with the specific purposes clearly described in the privacy statement, and on the basis of the lawfulness prerequisites that justify the processing (including consent where required);
- must be collected for specified, **explicit** and **legitimate purposes** and subsequently processed in ways that are not incompatible with those purposes ("*Purpose Limitation Principle*");
- must be **adequate**, **relevant** and **limited to what is necessary in** relation to the purposes for which they are processed ("*Principle of minimization*");
- must be **accurate** and, if necessary, **updated**;
- must be kept in a form that allows the identification of the data subjects **for a period of time not exceeding the achievement of the purposes** for which they are processed ("*Principle of Limitation of Retention*");
- must be processed in a manner that ensures **adequate security** of personal data, including protection--through appropriate technical and organizational measures--from unauthorized or unlawful processing and from loss, destruction, modification, disclosure or unauthorized access that could cause harm.

[1] Subsequent to the entry into force of the GDPR, on August 10, 2018, Legislative Decree No. 101/2018 on "*Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679*" was issued for the purpose of coordination with the previous Italian legislation.

Compliance with these principles is the responsibility of the **Data Controller** and involves **ongoing risk assessment**, **management** and **monitoring**.

All employees/collaborators of PCE are responsible for compliance with the principles and rules defined in this document.

Compliance with the provisions of this Policy should be considered an essential part of the contractual obligations of employees/collaborators.

Violations of this Policy may lead to **disciplinary action** including - in the most serious cases - dismissal, in accordance with applicable laws and labor contracts or termination of employment for third parties.

Compliance with the provisions of the law on the protection of individuals with regard to the processing of personal data, in addition to representing an approach in line with the principles incorporated in PCE's Code of Ethics constitutes, as well, an **important opportunity to rationalize, classify and order the personal data kept in the company according to updated criteria of necessity and security, limiting the duplication of excess data and avoiding the risks associated with the processing of the same.**

2.2 Definition of personal data

Personal data means **any information relating to an identified or identifiable natural person ("Data *Subject*"), directly or indirectly,** with particular reference to an identifier such as a name, an identification number, location data, an online identifier[2] or to one or more characteristic features of his or her physical, physiological, genetic, mental, economic, cultural or social identity[3] .

3. Privacy organizational model (P.O.M.)

3.1 Background

This section explains the **roles,** defined and actively involved in the management of the **Privacy Organizational Model (P.O.M.)**.

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

- Data **Controller**
- Holder**'s Delegate**
- **Data Processor** (Third Party)
- **Data Protection Officer**,
- **Authorized for** processing

[2] Online identifiers produced by devices, applications, tools (such as IP addresses, cookies, identification tags, etc.) can leave traces that, when combined with unique identifiers and other information received by the server, can identify individuals. Also included is the digital identification of the data subject, through authentication mechanisms (such as the same credentials used by the data subject to access - *log in* - to the online service offered by the Data Controller).

[3] The GDPR does not apply to the processing of **anonymous information**, i.e., *(i)* information that does not relate to an identified or identifiable natural person *(ii)* personal data rendered sufficiently anonymous that it prevents or no longer allows the Data Subject to be identified. Therefore, the Regulations do not apply to the processing of anonymous information for statistical or research purposes.

3.2 Data Controller

The Controller is the natural or legal person who, individually or together with others, determines the purposes and means of the processing of personal data.

3.3 Owner's Delegate

It is recognized that the Data Controller, in the person of the legal representative *pro tempore*, has the option to provide, under his own responsibility and within the framework of his own organizational structure, that **specific tasks and functions related to the processing of personal data be assigned to expressly delegated individuals, who operate under his authority**.

This, in order to better ensure technical-specialist oversight on the subject and a qualified internal division of tasks and functions.

The Data Controller's Delegate is, therefore, the natural person designated by the Data Controller and delegated to carry out the activities useful to ensure the constant and punctual compliance with the regulations in force regarding the processing of personal data, as well as to represent him/her in relations with interested parties and Authorities and in all acts and contracts appointing Third Parties.

The proxy, granted by special power of attorney, must be given adequate publicity, including internal publicity.

3.4 Processor (Third Party)

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

Personal data may be processed in the name and on behalf of the Data Controller by third parties, subject to the signing of an appropriate contract.

3.5 Third parties

When the processing is carried out by Third Parties, i.e. **suppliers, business associates or consultants who -** as natural or legal persons - **process personal data on behalf of the company Data Controller or Processor,** the performance of the processing is governed by a contract or other legal act obligating the Third Party to the Company and regulating the nature, purpose, 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 territory of the EU; the application of appropriate security measures and procedures; the obligations and rights of the Data Controller.

These individuals, expressly identified as "***Data Processors***" with a specific deed/contract of appointment (so-called "***Data Processing Agreement" or "DPA"***), will have to provide sufficient guarantees in terms of specialized knowledge, reliability and resources aimed at implementing adequate technical and organizational measures, including security, in order to ensure that the processing protects the rights of the Data Subjects.

The Processor may in turn use another responsible party (the ***SubResponsible Party***) with the **prior authorization of the Controller**.

In all cases, the SubResponsible person so designated by the Processor shall be bound by the same obligations set forth in the contract between the Controller and the Processor.

3.6 Authorized to process

Authorized Processors are the persons authorized to carry out personal data processing operations, who operate according to the written instructions provided by the Controller.

The Authorized Person shall limit the processing of personal data to **what is strictly necessary in** connection with the **performance of his or her duties** and in accordance with **the operational instructions received**, under the direct authority of the Owner.

For the purpose of responsible and lawful management, Authorized Processors who collect, use, and store personal data must:

- Maintain personal data accurately and up-to-date from collection to destruction;
- protect personal information so that it is not accessible to an indefinite number of people or otherwise to individuals who are not authorized or who do not have a valid reason for accessing the information;
- Prevent illegal or improper use of personal data;
- Ensure the traceability and retraceability of personal data (access, changes, storage) throughout its entire cycle;
- Retain personal data only as long as necessary for the stated purpose and/or as long as required by law;
- Promptly report any breach of Privacy (unauthorized access to systems, loss, theft, destruction or deletion of data) to the Data Controller;
- Avoid storing personal data on non-password-protected files and/or external storage or laptops, the loss or theft of which could result in a personal data breach ("Data Breach").

3.7 Authorized for video surveillance treatment

The Video Surveillance System Processing Authorized Person is the person who is authorized by the Owner/Manager to carry out **processing operations on the images, recorded and unrecorded, detected by the video surveillance systems installed at the Company's premises for the purpose of protecting the Company's assets.**

If, as part of a contract for surveillance services with the Company, a third party is authorized to carry out processing operations on behalf of PCE on the images collected by the video surveillance system, he or she must be appointed "Data Processor."

PCE carries out processing of personal data through video surveillance systems installed at its offices and facilities and are, therefore, required to adopt the applicable regulatory requirements for video surveillance.[4]

4. Record of treatment activities

In compliance with the provisions of the European Regulation PCE compiles the **Register of Processing Activities**.

[4] Data Protection Authority's Provision on Video Surveillance of April 8, 2010, as well as European Data Protection Board (EDPB) Guideline 3/2019 on Video Surveillance

The Register, prepared in written form, including in electronic format, is kept available to the competent authority.

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

5. Management model

Personal data processing operations must be carried out in a **lawful**, **fair** and **transparent** manner, strictly limited to what is necessary to pursue the purposes stated in the privacy policy and, in any case, compatible with those purposes.

Three stages of the "life cycle" of personal data can be identified:

- Collection;
- Treatment;
- Termination of Treatment and Cancellation.

5.1 Collection

5.1.1 Purpose

Processing of personal data (collected or received) by the ECP must be for the **pursuit of legitimate purposes**.

Personal data collected must be **adequate**, **relevant**, and **limited to** what is necessary for the purposes of their processing.

Some purposes are given below for illustrative purposes only:

- Customer and supplier relationship management;
- selection and recruitment of personnel and management of the employment relationship;
- Sending advertising materials and other promotional and marketing initiatives;
- sales activities;
- Access management at the Company's headquarters and video surveillance.

5.1.2 Legal Basis

Each processing of personal data requires identification of the **legal basis justifying the processing**, that is, the reason that legitimizes the processing of personal data.

Regarding personal data processed by PCE, the **legal bases** for processing are:

- **consent of the** data subject: when data processing is explicitly authorized by the data subject for one or more specific purposes (e.g., to use the data subject's data for marketing purposes)
- **the performance of a contract or pre-contractual provisions**: when the processing is necessary to fulfill a contract desired by the data subject (e.g., in order to ship products purchased by a customer, it will be necessary to collect his or her personal data such as first name, last name, address, etc.)

- **Compliance with a legal obligation**: when data processing is required by a law, regulation, etc. (e.g., in order to invoice a customer for the purchase of a good, it is necessary to collect the customer's tax data, etc.)
- **legitimate interest of the Data Controller**: when the processing is necessary for specific needs of the Data Controller provided that the processing is not excessively invasive for the data subject (e.g., to install a video surveillance system for security purposes).

5.1.2.1 Consent

Consent, where necessary as a **prerequisite for the lawfulness of processing**, must be expressed by a positive act by which the Data Subject manifests his or her **free**, **specific, informed** and **unambiguous intention** to accept the processing of personal data concerning him or her, either by **written** (including through electronic means, e.g., checking a box on a website) or **oral declaration.**

Silence, inactivity or pre-selection of boxes is not equivalent to giving consent.

Consent is considered **freely given** if the Data Subject is able to make a genuinely free choice and is in a position to refuse or withdraw consent without prejudice. Consent is presumed not to be freely given if:

- the performance of a contract, or the provision of a service, are conditional on the provision of consent that would not otherwise be necessary for the performance of that contract;
- or if separate consent cannot be given for separate processing of personal data.

In fact, it is necessary that **explicit consent for each specific purpose of processing** be sought in a comprehensible and easily accessible form. Where the processing has **more than one purpose**, consent must be given for each of them[5] .

Proof of the achievement of consent must be provided to the Data Controller (and/or the Processor), who must be able to prove that the Data Subject has expressly consented to the processing of the data.

In the case of **oral** collection of consent (e.g., in the performance of telephone marketing activities entrusted to *call centers*), the operators entrusted with the task of contacting lists of names and handling the telephone interview aimed at promotional activities and/or information gathering, will have to expressly use the *scripts* specifically prepared (for the Privacy Notice and Consent Collection), providing for the documentation of the consents that have taken place.

The consent of Data Subjects **is not necessary** for the performance of certain processing operations, namely:

- The performance of a contract to which the Interested Party is a party or execution of pre-contractual measures taken at the request of the Interested Party;

[5] Where processing for a purpose other than the purpose for which the personal data were collected is not based on the consent of the Data Subject, processing for the further and different purpose must be **compatible** with the purpose for which the personal data were initially collected (taking into account the link between the purposes, the context in which the data were collected, the nature of the data, the possible consequences of further processing, and the existence of appropriate safeguards).

- The fulfillment of a legal obligation to which the Holder is subject;
- the pursuit of the legitimate interest of the Data Controller, provided that the interests or fundamental rights and freedoms of the Data Subject do not prevail.

Some of the purposes for which specific consent must be obtained are mentioned below, merely by way of example:

- Sending advertising materials and other promotional and marketing initiatives;
- Profiling activities i.e., processing aimed at analyzing preferences, habits and consumption choices;
- activities concerning the processing of special categories of data, so-called **sensitive data** (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; genetic data; biometric data; data relating to a person's health or sex life or sexual orientation), as well as the processing of **personal data relating to criminal convictions and offenses**, where required by law.

Data Subjects have the opportunity to **revoke**, at any time, the consent previously given to the performance of certain processing operations.

In such cases, processing operations carried out pursuant to such consent must be **stopped immediately** unless there is some other legal basis for the processing (including, e.g., fulfillment of a legal obligation; defense of a right in court; conditions of legitimate interest of the Data Controller that are overridden by the interests, rights and fundamental freedoms of the Data Subject).

In all cases, consents and revocations must be appropriately tracked so that any changes/changes requested by Interested Parties can be documented.

5.1.2.2 Execution of a contract.

When the processing of personal data is **necessary** for the performance of a contract to which the data subject is a party or the performance of pre-contractual measures taken at the request of the data subject, the processing of personal data may be based on the legal basis of the performance of a contract.

Since the **criterion of necessity is** fundamental to this legal basis, data processing will be lawful only where the contract cannot be fully executed without the processing of personal data (e.g., for the purpose of signing a contract, the data subject's identification data must necessarily be requested). The data may be used only for the execution of the contract and not for other purposes such as, for example, marketing initiatives.

For processing based on this legal basis to be considered lawful, it will be necessary to **demonstrate**:

- The existence and validity of the contract between the company and the person concerned;
- The necessity of data processing for the execution of the contract.

It is always necessary to **provide the privacy policy** stating the legal basis for processing.

5.1.2.3 Fulfilling a legal obligation

This legal basis applies when the processing of personal data is necessary for the **fulfillment of obligations arising from the law**.

This is the case of processing of personal data necessary for the management of administrative, social security and tax obligations placed on companies in the context of labor relations (e.g., preparation of monthly pay slips, payment of social security contributions, etc.).

The legal obligation, however, must:

- be **established by law against the Data Controller**;
- Legal provisions must establish a **mandatory obligation to process personal data**, sufficiently clear and precise and must establish of the processing in question;

In these cases, the consent of the data subject is not required, but it is still appropriate to provide the privacy notice stating the legal basis for processing.

5.1.2.4 Legitimate interest

Where the processing of personal data is necessary for the pursuit of the **legitimate interest of** the Data Controller and provided that the interests or fundamental rights and freedoms of the data subject do not prevail, personal data may be processed without the prior consent of the data subject.

In order for processing to be based on this legal basis, however, a balancing between the interests of the Data Controller and the rights accorded to the data subject must be carried out in order to assess and prove the predominance of the interests of the Data Controller over the rights of the data subject.

In such a balancing act, it is necessary to consider:

- Whether the **processing is actually necessary** taking into account the **possible harm that** would result to the Controller if it were not carried out;
- the **impact on data subjects** and their **reasonable expectation of what** will happen to their personal data;
- The **presence of additional data protection measures** that may limit the impacts of processing on data subjects.

5.1.3 The privacy policy

The principles of fair and transparent processing imply that the Data Subject is informed of the existence of the processing and its purpose.

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

The manner in which personal data are collected, used, accessed or otherwise processed must be **transparent** to Data Subjects. In particular, the specific purposes for processing personal data must be **explicit** and **legitimate** and specified at the time of data collection.

The Privacy Notice must be provided to the Data Subject at **the time of collection of** the personal data or, if the data are obtained from another source, within a **reasonable period of time** but, at the latest,

within one month. Where personal data is intended for communication with the Data Subject or another recipient, the Privacy Notice must be provided no later than when the data is first communicated.

In the case of data collected directly from the Data Subject, the Data Subject must be informed of any obligation to provide personal data and the consequences of refusal to provide such data.

5.2 Treatment - General Principles

Processing operations carried out by PCE must follow the general principles dictated by the regulations and given below:

- ***Lawfulness, fairness and transparency***: data must be processed lawfully, fairly and transparently to the Data Subject;
- ***Purpose limitation***: data must be collected for specified, explicit and legitimate purposes, specifically stated and described clearly and comprehensibly in the Notice, and subsequently processed in ways that are not incompatible with those purposes. Use of collected data for purposes other than those stated in the Notice is not permitted: if the Data Controller intends to further process personal data for a purpose other than that for which it was initially collected, prior to such further processing it must provide the Data Subject with a new Notice and, if applicable, Data Subject must collect a new explicit consent;
- ***Data minimization***: data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- ***Accuracy***: data must be accurate and, if necessary, updated. All reasonable steps must be taken to correct or delete inaccurate personal data in a timely manner;
- ***Limitation of storage***: data must be kept in a form that allows the identification of the Data Subject for a period of time not exceeding that necessary to achieve the purposes for which it was processed;
- ***Integrity and Confidentiality:*** data must be processed in a manner that ensures adequate security of personal data, including protection-through appropriate technical and organizational measures-from unauthorized or unlawful processing and from loss, destruction, modification, disclosure, or unauthorized access that could cause harm.

5.2.1 Processing by Third Parties

Processing of personal data by Third Parties means all instances in which data owned by PCE, or for which PCE has been designated as a Data Processor, are made accessible in any way, including by remote connection, to Third Parties.

In these cases, the provisions of Section 3.5 will apply.

5.2.2 Cross-border transfers of personal data

With cross-border transfers of personal data outside the EU/EEA there may be an increased risk that the Data Subject may not be able to exercise his or her right to data protection, particularly to protect against unlawful use and disclosure of such information.

It is appropriate that when personal data are transferred from the EU/EEA to Data Controllers or Processors in third countries (outside the EU/EEA), the level of protection of individuals ensured within the EU by the European Regulation should not be compromised, even in cases of subsequent transfers of personal data from the third country to other third countries.

The transfer of personal data to a third country (to be understood as any case in which the data is accessible in a foreign state, including by simple remote access) may take place only for the purpose of pursuing the purpose communicated to the Data Subject at the time of collection and in accordance with the specific provisions regarding the transfer of personal data abroad.

The transfer to a third country of personal data that are subject to processing or are intended to be subject to processing after the transfer may be made to countries that - upon a decision of the European Commission - guarantee an adequate level of protection (transfer on the basis of an **adequacy decision**).

In the absence of an adequacy decision, and except in cases where the transfer is permitted by law (including the unambiguous consent of the data subject; the necessity of the transfer for the performance of contractual/pre-contractual measures the necessity of the transfer for the exercise or defense of a right in a court of law), the Data Controller must provide to compensate for the lack of protection, related to the transfer of personal data to third countries, with **adequate safeguards** to protect Data Subjects, including the availability of enforceable rights of Data Subjects and effective remedies, through alternatively:

- **Binding Corporate Rules** (*BCRs*), approved by a supervisory authority, aimed at allowing the transfer of personal data from the territory of the state to third countries between companies belonging to the same business group. They take the form of a document containing a series of clauses (*rules*) setting out the *binding* principles to which all companies belonging to the same (*corporate*) group are obliged to comply [6] ;
- *Standard Contractual Clauses (SCCs) adopted by* the Commission or adopted by a supervisory authority and approved by the Commission;
- **Model (ad hoc) contract clauses** authorized by a supervisory authority;
- **Codes** of conduct are rules of conduct or uniform practices developed by various international bodies or even by individual states, intended to contribute to the proper implementation of the Regulations, depending on sectoral specificities and the specific needs of micro, small and medium-sized enterprises.
- **Certification mechanisms** are forms of accreditation that make it possible to obtain the issuance of an attestation from a third party (certification body - CB) for the purpose of demonstrating the compliance, with the General Data Protection Regulation (GDPR), of the processing carried out.

[6] BCRs constitute a mechanism that can simplify the burdens on multinational companies with regard to intra-group flows of personal data. In fact, the issuance of an authorization (by the Garante per la protezione dei dati personali) to the transfer of personal data (from Italy to third countries) through Binding Corporate Rules allows the companies of the multinational group that has requested it, even if they are established in different countries, to transfer personal data within the corporate group without the need for further requirements, provided that they comply with what is established within the text of the BCRs and only for the purposes indicated therein.

[7] A number of burdens are placed on the multinational group that makes use of BCRs, including: setting up a staff training program on personal data protection; implementing a mechanism for handling litigation and reports related to BCRs; conducting periodic audits in order to verify compliance with BCRs by Group companies; and establishing a staff to monitor compliance with BCRs and handle reports from Data Subjects.

5.2.3 Cookies and similar technologies

The PCE website may use *cookies* or technologies assimilated to them for **profiling and marketing** activities, in particular in order to analyze or predict aspects regarding the Data Subject's preferences, habits or consumption choices or personal interests and to provide targeted advertising services or content, display content and propose commercial initiatives.

Cookies, except those necessary that enable the normal operation of the websites, can be used with the consent of the data subjects. Consent is acquired through the opening of a banner visible to users on their first visit to the site by which interested parties are invited to express their preferences regarding the use of cookies, so-called **cookie manager**.

The cookie manager, in addition to allowing users to provide or deny consents for categories of cookies also allows them to have granular information about categories of cookies i.e. in relation to each individual cookie such as purpose of the cookie, duration, category (technical, analytical, marketing, profiling).

Consent, where provided, is acquired in a lawful manner (see section 5.1.3 on consent for its validity requirements) and is tracked to document the data subject's choice.

5.2.4 Security

As part of the processing operations carried out, PCE implements measures to ensure a **level of security appropriate to the risk**.

In particular, personal data must be processed in a manner that ensures **adequate security** including protection-through appropriate technical and organizational measures-from unauthorized or unlawful processing and from loss, destruction, modification, disclosure, or unauthorized access.

Taking into account the state of the art, the costs of implementation in relation to the risks posed by the processing operations, and the nature of the personal data to be protected, the following measures in particular are implemented:

- Physical access controls;
- Restrictions to authorized personnel only for specific sensitive areas (HR file, Control Room, video surveillance systems);
- Secure destruction of paper records containing personal data;
- Secure deletion of computer media that, used for data processing, are intended for other use;
- Timely restoration of availability and access to personal data in the event of a physical or technical incident;
- Implementation of measures to protect the networks, systems and software with which personal data are processed;
- Application of the principle of Privacy by *design* and *by default* (see Section 7) in the design of systems and the design of business processes and procedures**;**
- processes, tools and organization to ensure timely reporting of any unlawful attempts to access personal data;
- Procedures for handling breaches (Data Breach);
- Adoption of solutions for tracking activities performed on personal data;

- Adequate operational practices to regularly test, verify and evaluate the effectiveness of technical and organizational measures to ensure the security of processing.

5.3 Specific Treatments - Termination of Treatment - Deletion and Destruction

PCE:

- takes all reasonable steps to **delete or rectify in a timely manner data that are inaccurate** with respect to the purposes for which they are processed;
- ensures that the **period of retention of personal data is limited to the minimum necessary in** relation to the specific purposes of collection and processing.

In order to ensure that personal data are not kept longer than necessary, a **time limit for termination of processing and deletion** should be established.

This period is stated as ten years, coinciding with the ordinary limitation period for rights arising from contractual relationships established by the Company.

6. Rights of the data subject and feedback

The Data Subject has the right to access the personal data concerning him or her and to exercise this right easily, to be aware of the processing and to verify its lawfulness.

In particular, every Interested Party has the right to know and obtain communications in relation to:

- To the purposes for which and the period during which personal data are processed;
- To recipients of personal data;
- to the logic to which any automated data processing responds and the possible consequences of any profiling.

PCE facilitates and cannot refuse to comply with the request to exercise the rights of the Data Subjects, unless it proves that it is unable to identify the Data Subject.

The interested party must be provided with the requested information **without undue delay** and, at the latest, **within one month of** receipt of the request, unless an extension is granted - in cases permitted by law - taking into account the complexity and number of requests.

The rights of the Data Subjects under the data protection legislation are set out below.

6.1 Right of access

The Data Subject has the right to obtain confirmation as to whether or not personal data concerning him or her are being processed and, if so, to obtain access to and a copy of the data being processed.

6.2 Right of Rectification

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

6.3 Right to cancellation

The Data Subject has the right to obtain the deletion of personal data concerning him or her, and the Data Controller is obliged to delete them without undue delay if any of the following reasons exist:

- personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the Data Subject withdraws the consent on which the processing is based and there is no other legal basis for the processing (including, e.g., fulfillment of a legal obligation; defense of a right in court; conditions of legitimate interest of the Data Controller that are overridden by the interests, rights and fundamental freedoms of the Data Subject);
- the data subject objects to the processing of personal data concerning him or her;
- Personal data are processed unlawfully.

6.4 Right to restriction of processing

The Data Subject has the right to obtain restriction of processing when, among other cases:

- disputes the accuracy of personal data, for the period necessary for the Data Controller to verify the accuracy of such data;
- when, in the face of unlawful processing, the Data Subject objects to the deletion of personal data and instead requests that their use be restricted.

Ways of restricting the processing of personal data may be to temporarily transfer selected data to another processing system, or to make selected personal data inaccessible to users, or to temporarily remove published data from a website.

6.5 Right to data portability

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

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

When exercising his or her rights with regard to data portability, the Data Subject has the right to obtain the direct transmission of personal data from one Data Controller to another, if technically feasible. Where a certain set of personal data concerns more than one data subject, the right to data portability must not affect the rights and freedoms of other data subjects.

6.6 Right of Objection

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

The exercise of this right results in the abstention from further processing of personal data, unless it is demonstrated that there are compelling legitimate grounds for processing that override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defense of a legal claim.

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

6.7 Response to the applicant and deadlines

Prior to the response to the exercise of rights, it is essential that the Group Company take all reasonable measures to verify the identity of the Data Subject, or of the person making the request on their behalf, particularly in the context of online services or online identifiers, by requesting - where appropriate - a copy of a valid identity document.

If the request comes from a person acting on behalf of the person concerned, it is necessary to check:

- The proxy signed by the Interested Party;
- The identity of the Data Subject and the delegated person.

If the request concerns access to the data of a deceased person, it is necessary to identify the requester and ascertain that he/she is an heir, or otherwise, a person entitled to exercise the right. It is appropriate to trace the response provided to the Data Subject or the person delegated by him/her.

7. Privacy by design & by default

The principle of accountability requires the Data Controller to be able to demonstrate compliance with the GDPR through the adoption-from the conception stage of the apprestate measures ("***Privacy by design***")-of appropriate technical and organizational measures and directives to ensure that only the personal data necessary (in terms of quantity, scope of processing, retention period, and accessibility) for each specific purpose of processing are processed by default ("***Privacy by default***").

These measures must minimize the processing of personal data, pseudonymize personal data as quickly as possible, allow Data Subjects control over the processing of their data, improve security levels, and define the responsibilities of all those involved.

In order to implement design solutions for personal data processing, processes and information systems that can protect data during all phases of the "life cycle," PCE implements technical and organizational measures to preventively ensure its protection, complying with the following rules:

- responsibility for data processing by all PCE employees;
- Information to Data Subjects about how PCE collects, uses, stores, and discloses personal data;
- Use and storage of data exclusively for the purposes declared to the Data Subjects and expressly authorized;
- Transfer of data to parties in a business relationship only for the purposes identified in the disclosure and that ensure an adequate level of security;
- Limited access to data by authorized personnel trained in handling personal data;
- Periodic verification regarding the proper application, both internally and externally, of the principles and guidance provided in this Policy.

The Privacy by Design and by Default approach must consider the entire "lifecycle" of personal data, from collection to deletion, in relation to any recording, storage, consultation, use, communication, and transfer operations.

8. Data protection impact assessment (DPIA).

When a type of processing, particularly if it involves the use of new technologies or is of new application, presents a **high risk** to the rights and freedoms of Data Subjects, PCE- **prior to the processing** itself- conduct a **personal data protection impact assessment** to determine the likelihood and severity of that risk taking into account all the circumstances of the processing.

The result of the assessment must be used to determine the measures and safeguards to be taken to reduce risk in compliance with the GDPR.

Where such identified measures are not practically adoptable, due to available technologies or implementation costs, the supervisory authority will need to be consulted before treatment activities begin.

The impact assessment must cover the entire lifecycle of the data collected and must be updated periodically or in any case whenever it is necessary because of the time that has elapsed since the initial processing. or because of significant changes in the processing in the type of data processed, the processing methods, or the technological solutions employed that result in a significant change from the previous analysis.

Impact assessment is, however, mandatory:

- in the case of automated processing, including profiling, on which decisions are based that have legal effects or similarly significantly affect Data Subjects;
- in case of processing, on a large scale[8] , of special categories of personal data that present a high risk to the rights and freedoms of Data Subjects;
- In the presence of the large-scale systematic surveillance of a publicly accessible area.

9. Data transfer impact assessment (TIA).

When processed personal data are to be transferred to Third Parties located in countries outside the EU/EEA that do not offer an adequate level of protection or protection equivalent to that provided by the GDPR, a Transfer Impact Assessment" or "TIA" must be carried out.

This assessment analyzes the legislation in force in the country of transfer and the risks to the rights and freedoms of data subjects, taking into account the nature, scope, context and purposes of the processing.

PCE must document the transfer impact assessment process and, when requested, to make it available to the relevant supervisory authority.

[8] Large-scale processing aims at the processing of a significant amount of personal data which, since it may affect a large number of Data Subjects, can potentially present a high risk to the rights and freedoms of Data Subjects.

The outcome of the assessment will need to be taken into account when determining what **further measures** and safeguards need to be taken for risk mitigation and compliance with the provisions of the GDPR.

10. Notification in case of personal data breach

A data breach (Data ***Breach***) must be addressed appropriately and promptly in order to avoid or limit causing harm to Data Subjects, such as: loss of control of personal data; discrimination, identity theft or usurpation; financial loss; injury to reputation; loss of confidentiality of personal data protected by attorney-client privilege; or any other significant harm to the natural person concerned.

Therefore, in cases of personal data breaches, PCE who suffered the breach must:

- Verify that all appropriate technological and organizational protective measures have been put in place according to the breach;
- notify the competent supervisory authority of the event without undue delay and, where possible, within 72 hours of learning of it.

The Data Breach Procedure for proper handling of security incidents related to personal data is as follows.

By way of example and not limitation, events of possible personal data breach may consist of:

- **Irretrievable loss of data (whether in electronic or paper format)** i.e. the inability to restore the data. For example, in cases of loss/theft of computer media or fire/flooding of paper archives;
- **Unauthorized access to data (computer systems or paper archives)** i.e. violation of the confidentiality of the data contained in the same systems or archives in cases of cyberattack through exploitation of vulnerabilities in the systems or misuse of authentication credentials, consultation of paper archives whose access is allowed only to authorized personnel;
- **Loss of data integrity** i.e. irreparable impairment of the correctness, congruence and consistency of data. In cases of unauthorized modification of data, human error, computer-related incidents;
- **Revelation or disclosure of data (whether in electronic or paper format) to unauthorized third parties**, including unidentified ones, such as through e-mail or even verbally.

As soon as the personal data breach is known, the person who has become aware of it should promptly report it to the Data Controller.

In the event that the event is indeed deemed to be a Data Breach, the Data Controller will take the necessary corrective measures (Data Breach mitigation activities) and, unless the breach is unlikely to present a risk to the rights and freedoms of the Data Subjects, will notify the competent supervisory authority of the established breach **without undue delay** and, where possible, **within 72 hours of becoming aware of it.**

In the event that the violation exposes the Data Subjects to **high risks**, the Controller will send, without delay, a direct communication to each of them, describing the nature of the established violation.

11. Inspections by the supervisory authority

The relevant supervisory authorities may conduct inspections at the Company aimed at verifying the Company's effective enforcement of the provisions of the law.

In the course of such inspections, PCE will adopt the precautions and safeguards provided for in internal regulations concerning relations with public supervisory authorities.

Documents or information related to the processing of personal data may be handed over to inspectors only with the authorization of the Sole Administrator, who must attend the inspection visit.

12. Training

The privacy training plan (courses, recipients, timing) is defined by the Data Controller.

The purpose of the training is to train and inform those authorized to process on:

- Regulations and Measures of the Privacy Guarantor;
- Type of data and processing methods;
- Privacy management model implemented;
- roles and responsibilities;
- disclosure, access rights, complaints and sanctions;
- security measures taken.

In cases of new hires, job changes, or the introduction of significant new tools relevant to the processing of personal data, the training must be updated be updated and delivered in a reasonably short time.

13. Sanctions

Violation of data protection regulations may expose PCE to different types of liability and consequent sanctions (administrative and/or criminal) depending on the rules concretely violated and to negative consequences on the company's reputation, including significant ones.

Failure to comply with the obligations set forth in this Policy constitutes conduct that is relevant for disciplinary purposes and may result in the application of the disciplinary sanctions provided by applicable laws and labor contracts.