M-Cube Group

Privacy Policy

DOCUMENT CLASSIFICATION	internal
DOCUMENT REF	ISMS-PLS-A18
APPROVED BY	CEO

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1	14/11/2022	Alexandre Lienard	First release
2	18/12/2023	Andrea Ceiner	updated to ISO 27001:2022
3	08/07/2024	Andrea Ceiner	Added Annex 1 and Annex 2

	Privacy Policy
	ISMS-PLS-A18

Summary

1. Introduction and definitions

This document is one of the components of the Security Referential which brings together all the standard rules that must be applied to guarantee, in a coherent and effective manner, the organization privacy and security policy.

In this Privacy Policy, the following terms have the meanings ascribed to them:

- "Data controller" (aka “Owner”) means the entity that determines the purposes and means of processing personal data.
- "Data processor" refers to any person or entity that processes personal data on behalf of the data controller.
- “Data Subjects” refers to the natural person to whom the Personal Data refers.
- “M-Cube Organization” refers to M-Cube S.p.A. - Via San Galdino,6 - 20154 Milano (Italy), that is the data controller responsible for the processing of personal information collected through its products and services and software applications.
- “Owner” refers to M-Cube Organization, as Data Controller, contactable via e-mail to **privacy@mcubedigital.com**.
- "Personal data" refers to any information relating to an identified or identifiable natural person (data subject).
- “Users” refers to Data Subjects using products, services or software applications provided by M-Cube Organization.

2. Scope of application and objectives

This document is part of the information security reference system and applies to all the organization staff members as well as to its subcontractors required to process personal data on its behalf (e.g. external consultants).

This policy focuses on aspects relating to the protection of privacy and is not an exhaustive compendium of all applicable legislation and rules.

However, the data Owner should be contacted for all questions, requests and/or doubts relating to these aspects.

3. Document Management

This document is managed in accordance with the ISMS document management policy.

This document comes into force from its publication and its distribution to the parties concerned.
The security requirements described in this document are, if necessary, broken down into operational procedures.

ANNEX 1: APPOINTMENT AS A PERSON OF M-CUBE IN CHARGE OF THE PROCESSING OF THIRD-PARTY PERSONAL DATA
When M-CUBE is in business relationship with an external legal entity (Third-Party), and M-Cube has to process/store by its own applications/systems the Third-Party's personal data, than annex 1 of this document has to be compiled and signed off by both parties.

ANNEX 2: APPOINTMENT AS AN EXTERNAL PERSON IN CHARGE OF THE PROCESSING OF M-CUBE'S PERSONAL DATA
When M-CUBE is in business relationship with an external legal entity (Third-Party), and the Third-Party has to process/store by its own applications/systems the M-CUBE's personal data, than annex 2 of this document has to be compiled and signed off by both parties.

3.1 Audience

This document concerns all employees, as well as subcontractors working on behalf of the organization.

3.2 Reference Documents

This document is based on:

Designation	Description
ISO 27001 :2022	Standard specifying the requirements for establishing, implementing, updating and continuously improving an information security management system in the context of an organization.
ISO 27002:2022	Standard defining the guidelines relating to best practices in information security management. These guidelines are embodied in a set of security measures to be implemented as part of the process of implementing the information security management system. Especially the Clause A.5.34 Privacy and protection of PII (personal identifiable information).

3.3 Changes to this privacy policy

The Owner reserves the right to make changes to this privacy policy at any time by notifying its Users possibly within the Owner's Website and/or - as far as technically and legally feasible - sending a notice to Users via any contact information available to the Owner.
Should the changes affect processing activities performed on the basis of the User's consent, the Owner shall collect new consent from the User, where required.

4. Data types and treatment register

Personal Data Types treatment is recorded into the Register.

In the event of incorrect personal data, the inaccuracy should be communicated to the data Owner, so that the errors can be corrected in the Register.

4.1 Types of Data collected

Users' personal information is collected when voluntarily provided, such as when filled out into digital or paper forms.
The data types of personal information collected are:

- Contact information (e.g., name, email address, phone number)
- Demographic information (e.g., age, gender)
- Billing address
- Suppliers' bank accounts for payments
- Usage data (e.g., IP address, browser type, referring website, pages visited).
- Account credentials (username and password).

5. Data Processing

5.1 Purposes of processing

The Data concerning the User is collected to allow the Owner to provide its Service, comply with its legal obligations, respond to enforcement requests, protect its rights and interests (or those of its Users or third parties), detect any malicious or fraudulent activity, as well as the following: Contacting

the User, Managing contacts and sending messages, Interaction with external social networks and platforms, SPAM protection, Analytics, Displaying content from external platforms, Tag Management and Remarketing and behavioral targeting.

Personal data must be processed fairly, lawfully, and transparently with regard to the person concerned. On the one hand, the clauses relating to respect for the privacy of the persons concerned must be easily accessible and clearly legible for the persons concerned. On the other hand, the inconvenience caused to the data subjects must be proportionate to the legitimate interest of the controller.

The personal information is collected for the following purposes:

- To provide and improve our services;
- To respond to inquiries, requests, or support needs;
- To personalize user experience and deliver relevant content;
- To process payments and fulfill orders;
- To send periodic emails or newsletters;
- To conduct research and analytics;
- To comply with legal obligations.

Personal data should only be collected, used or disclosed for the purposes disclosed to the individual and any purpose authorized by the individual therefor. In some cases, personal data may be used or disclosed to notify the individual, as necessary, to comply with a legal obligation, to assert, defend or investigate a right, or to satisfy an obligation imposed by a public authority.

Personal data collected for a purpose may only be further processed in a manner compatible with the purpose for which it was obtained.

5.2 Processing of sensitive personal data

The processing of sensitive personal data is in principle prohibited. The processing of sensitive personal data is only permitted exceptionally in the following cases:

- When necessary for the performance of specific labor law obligations and rights;

- When it is necessary for the establishment, exercise or defense of a legal right, for example, in the event of legal proceedings on the grounds of discrimination.

The processing of data concerning a person's health is in principle prohibited, except for exceptions exhaustively listed in the law, including in particular:

- A processing of data relating to health necessary within the framework of the exercise of rights and obligations of the organization in terms of labor law
- The application of social security, for example, for the management of maternity leave or the management of occupational medicine.

In all cases where the processing of data concerning health is authorized, the processing of this data is subject to additional obligations, including that of keeping up to date a list of the categories of persons having access to this data, specifying their functions. The persons who process these transactions are bound by an enhanced duty of discretion.

The processing of judicial data is in principle prohibited with the exception of the following cases:

- When processing is necessary for the achievement of purposes set by law, for example in the case of data relating to suspected money laundering.
- Where the processing is required by lawyers or legal advice.

The processing of judicial data is subject to additional obligations, including that of keeping an up-to-date list of the categories of persons having access to this data within the company, specifying their functions. The persons who process these transactions are bound by an enhanced duty of discretion.

The collection and processing (including the mere mentioning) of the national ID is in principle not permitted, unless authorization is granted by the CNIL, a division of the Commission for the Protection privacy, or on the basis of specific regulations, for example in the area of consumer credit or under social security obligations. The possible consent of the persons concerned does not make it possible to lift this prohibition in principle.

5.3 Data Place & Transfer

The Data is processed at the Owner's operating offices and in any other places where the parties involved in the processing are located.
Depending on the User's location, data transfers may involve transferring the User's Data to a country other than their own.
We ensure that any data transfer outside the European Economic Area (EEA) is done in compliance with the GDPR requirements.
Users are also entitled to learn about the legal basis of Data transfers to a country outside the European Union or to any international organization governed by public international law or set up by two or more countries, such as the UN, and about the security measures taken by the Owner to safeguard their Data.
If any such transfer takes place, Users can find out more by inquire with the Owner using the information provided in the contact section.

5.4 Retention time

Personal Data shall be processed and stored for as long as required by the purpose they have been collected for.
Therefore:

- Personal Data collected for purposes related to the performance of a contract between the Owner and the User shall be retained until such contract has been fully performed.
- Personal Data collected for the purposes of the Owner’s legitimate interests shall be retained as long as needed to fulfill such purposes. Users may find specific information regarding the legitimate interests pursued by the Owner within the relevant sections of this document or by contacting the Owner.

The Owner may be allowed to retain Personal Data for a longer period whenever the User has given consent to such processing, as long as such consent is not withdrawn. Furthermore, the Owner may be obliged to retain Personal Data for a longer period whenever required to do so for the performance of a legal obligation or upon order of an authority.
Once the retention period expires, Personal Data shall be deleted. Therefore, the right of access, the right to erasure, the right to rectification and the right to data portability cannot be enforced after expiration of the retention period.

5.5 Data Security

The organization undertakes to adopt technical and organizational measures to ensure the security of the data it processes. These measures, defined in the organization's information security repository, aim in particular to:

- Limit access to data and processing possibilities to what people need for the exercise of their function or for the needs of their service;

- Ensure compliance of the operations carried out with the information included in the clause on the protection of privacy and in the declaration provided to the commission for the protection of privacy;
- Protect data against destruction, loss, falsification, dissemination or unauthorized access;
- Ensure the obligation of data confidentiality;
- Set a data retention period and ensure that it is respected.

5.6 Data Sharing and Disclosure

Personal data could be shared with

- affiliated companies, subsidiaries, and third-party service providers necessary for the provision of services.
- Law enforcement agencies, regulatory bodies, or government authorities when required by law or to protect data Owner's rights.
- Other third parties with consent of the User.

Any data transfer outside the European Economic Area (EEA) is done in compliance with the GDPR requirements.

5.7 Consent

Consent for a data subject is excplicitly requested when needed, and recorded.

In the case of a child under the age of 16, the consent of the legal representative is mandatory.

5.8 Legal basis of processing

The Owner may process Personal Data relating to Users if one of the following applies:

- Users have given their consent for one or more specific purposes. Note: Under some legislations the Owner may be allowed to process Personal Data until the User objects to such processing ("opt-out"), without having to rely on consent or any other of the following legal bases. This, however, does not apply, whenever the processing of Personal Data is subject to European data protection law;
- provision of Data is necessary for the performance of an agreement with the User and/or for any pre-contractual obligations thereof;

- processing is necessary for compliance with a legal obligation to which the Owner is subject;
- processing is related to a task that is carried out in the public interest or in the exercise of official authority vested in the Owner;
- processing is necessary for the purposes of the legitimate interests pursued by the Owner or by a third party.
- In any case, the Owner will gladly help to clarify the specific legal basis that applies to the processing, and in particular whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract.

6. Duty to inform

A duty to inform the persons concerned must be implemented in order to ensure transparency with regard to them as to the processing which is or will be carried out with their personal data.

When collecting personal data, the data subject must be informed, via a privacy clause, of the data processing activities, unless this prevents the data controller from observing a legal obligation, to exercise a legal right or to comply with the orders of public authorities.

The person responsible for processing personal data is obliged to communicate the following data to the data subject:

- The identity of the person or company collecting the data;
- The name and address of the controller;
- The purposes of the processing;
- The types of third parties to whom the data may be communicated and/or disclosed;
- The existence of a right of access to data and a right to rectify incorrect data.

7. Incident notification

Each employee, temporary or contract worker, supplier and other subcontractor who processes personal data for the organization or on its behalf, must immediately contact the data Owner in the event of an incident or breach of privacy.

7.1 Data leak

Personal data leak shall be detected, reported and analyzed.

8. Rights of the Users

Users may exercise certain rights regarding their Data processed by the Owner.
In particular, Users have the right to do the following:

- **Withdraw their consent at any time**. Users have the right to withdraw consent where they have previously given their consent to the processing of their Personal Data.
- **Object to processing of their Data.** Users have the right to object to the processing of their Data if the processing is carried out on a legal basis other than consent. Further details are provided in the dedicated section below.
- **Access their Data.** Users have the right to learn if Data is being processed by the Owner, obtain disclosure regarding certain aspects of the processing and obtain a copy of the Data undergoing processing.
- **Verify and seek rectification**. Users have the right to verify the accuracy of their Data and ask for it to be updated or corrected.
- **Restrict the processing of their Data**. Users have the right, under certain circumstances, to restrict the processing of their Data. In this case, the Owner will not process their Data for any purpose other than storing it.
- **Have their Personal Data deleted or otherwise removed**. Users have the right, under certain circumstances, to obtain the erasure of their Data from the Owner.
- **Receive their Data and have it transferred to another controller**. Users have the right to receive their Data in a structured, commonly used and machine readable format and, if technically feasible, to have it transmitted to another controller without any hindrance. This provision is applicable provided that the Data is processed by automated means and that the processing is based on the User's consent, on a contract which the User is part of or on pre-contractual obligations thereof.
- **Lodge a complaint**. Users have the right to bring a claim before their competent data protection authority.

8.1 Details about the right to object to processing

Where Personal Data is processed for a public interest, in the exercise of an official authority vested in the Owner or for the purposes of the legitimate interests pursued by the Owner, Users may object to such processing by providing a ground related to their particular situation to justify the objection. Users must know that, however, should their Personal Data be processed for direct marketing purposes, they can object to that processing at any time without providing any justification. To learn, whether the Owner is processing Personal Data for direct marketing purposes, Users may refer to the relevant sections of this document.

8.2 How to exercise these rights

Any requests to exercise User rights can be directed to the Owner through the contact details provided in this document. These requests can be exercised free of charge and will be addressed by the Owner as early as possible and always within one month.

9. Subcontracting management

The transfer and disclosure to third parties must comply with the principles relating to the protection of personal data. The level of protection of personal data offered by these third parties must therefore be at least of the same level as that offered by the organization. In any case, appropriate protection should be offered to all personal data processed by the organization in accordance with the law and the commitments made to the data subjects.

10. Training and awareness

In accordance with the human resources security policy, the organization must provide the necessary data protection training to any member of staff who has access to personal data in the performance of their duties. The organization must also make its personnel aware of the issue of protection of personal data.

11. Protection of privacy

The organization implements technical and organizational measures that respect the principles of:

- "Privacy by Design" aimed at ensuring that the protection of privacy is taken into account, in a preventive and proactive manner, from the design and within the operation of information systems as well as in the implementation of internal practices.
- 'Privacy by Default" aimed at guaranteeing that, by default, an automatic and implicit protection of personal data. These measures cover in particular the amount of personal data collected, the extent of their processing, their retention period and their accessibility.

11.1 Applicability

The principles of "Privacy by Design" and "Privacy by Default" must be taken into consideration for any information system project involving the processing of personal data. These principles must also be taken into account in the context of public procurement.

11.2 Respect the interests of data subjects

The interests of the persons concerned must be protected during the design, in particular by providing for strict and implicit measures to protect privacy, in accordance with the expectations of the persons concerned and with the legal requirements. This requirement places the protection of the personal data of the persons concerned at the center of all considerations.

11.3 Proactive and preventive measures

Privacy must be considered throughout the life cycle of the personal data processing process. In particular, proactive and preventive measures must be considered upstream in order to anticipate and prevent incidents of privacy breaches before they occur.

11.4 Default, implicit and automatic protection

In accordance with the principle of "Privacy by Default", data subjects should be allowed to have their personal data:

- Are systematically protected within the information systems or within the framework of internal practices;
- Benefit from the highest level of maximum protection without any intervention on their part.

Mechanisms must be implemented to ensure that, by default, only the personal data necessary for each specific purpose of the processing will be processed. These data are not, in particular, collected or stored beyond the minimum necessary for these purposes, in terms of both the quantity of data and the duration of their storage.

Mechanisms must be implemented to ensure that, by default, personal data is not made accessible to an indeterminate number of natural persons.

Anyone involved in the life cycle of an information system processing personal data, including in particular developers, project managers and information system managers, is responsible for applying the principle of "protection of privacy by default" aimed at guaranteeing an automatic and implicit protection of personal data.

11.5 Data protection by design and at the heart of practices

In accordance with the principle of “Privacy by Design”, protection of privacy must be integrated from the design stage and within the architecture of information systems and internal practices. Protection of privacy must therefore be an essential element of the basic functionalities and must be an integral part of the information systems, without impairing their functionalities.

The implementation of the principle of "Privacy by Design" must take into account all the legitimate interests and objectives of the organization and must not prejudice them. Privacy by design avoids these false dichotomies, such as that between privacy and security, by demonstrating that it is indeed possible to achieve both objectives at the same time.

The principle of "Privacy by Design" must be considered by all the personnel of the organization as a real added value allowing in particular to maintain the parameter of user trust, a major element in the relationship with them. It is everyone's responsibility to ensure the integration and proper dissemination of this principle.

END.

ANNEX 1: APPOINTMENT AS A PERSON OF M-CUBE IN CHARGE OF THE PROCESSING OF THIRD-PARTY PERSONAL DATA

The undersigned [Name Surname], in his capacity as legal representative of **"[name of THIRD-PARTY ORGANIZATION]",** with registered office in via [Address], Registration Number in the [city] Business Register and Tax Code no.[number]- Tel: [tel], E-mail: [e-mail address]; PEC: [pec address]- Data Controller pursuant to EU Regulation 2016/679,

NOMINATION

"**M-Cube SPA**" - legally represented by Mr. Manlio Romanelli, with registered office in via San Galdino n.6, 20154, Milan, Registration Number in the Milan Business Register and Tax Code no.01022540320- Tel: 040634364, E-mail: info@mcubedigital.com; PEC: mcube@pec.it - in charge of the processing of personal data, by apponting to this responsibility Mr. Alberto Vitulano (c.f. VTLLRT72H26A022C), born in Cermes (BZ), in date 26/06/1972 having address at the working site of MCUBE SPA in Via S. Galdino 6, Milano. In order to correctly apply EU Regulation 2016/679 (hereinafter also referred to as the "Regulation") and to adequately protect the rights of the Data Subjects, the following operations will be carried out:

- ensure and ensure that all customers and suppliers falling within the scope of the GDPR have signed the consent to the processing of data and have received the information on the processing of data;
- ensure and ensure that all external Managers have signed the appointment in relation to their specific tasks and for the authorized purposes;
- take care of the updating of the List of External Managers;
- support the subsidiaries (branches) in the adoption and implementation of the Group Privacy Policy, also by making use of external professionals;
- analyze whether there are new processes that may lead to a change in risk in data processing;
- communicate the results of the aforementioned analysis to the Group's "Compliance" organisational function (privacy@mcubedigital.com);
- immediately notify the Group's "Compliance" (privacy@mcubedigital.com) organisational function of any data breaches and provide immediate support in the management of these cases.

With this act of appointment, in compliance with the provisions of the Regulations, it is provided that:

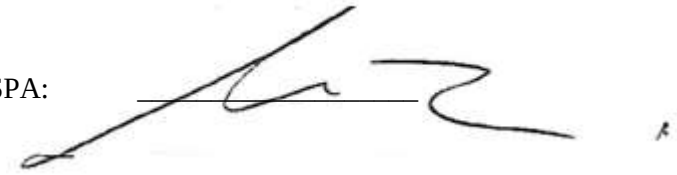
1. all the data of which the Person in Charge becomes aware by reason of his role, task, company function, are processed by the Person in charge exclusively for the performance of his or her work on behalf of the Data Controller, for the time strictly necessary;
2. it is not permitted to communicate such data to third parties, unless the communication is essential for the performance of the work of the Person in Charge and takes place towards third parties authorised by the Data Controller, in the manner provided by the latter;
3. the Person in charge processes personal data in compliance with the principles of lawfulness, fairness, transparency, only for the purposes for which such data were collected (so-called purpose limitation) and only to the extent necessary for the pursuit of these purposes (so-called processing minimization);
4. the personal data processed must be accurate and, if necessary, updated and stored for the time strictly necessary to pursue the above purposes (so-called storage limitation);
5. the Data Processor processes the data following the instructions given by the Data Controller in order to ensure adequate security of the personal data processed, as well as respect for the rights and freedoms of the data subjects;
6. the Data Controller informs the Data Processor of the privacy policies adopted, which are always available to the Data Processor for consultation. Please refer to the policy document for any instructions to be followed in the processing of personal data;
7. the Person in Charge is authorised to transmit data within the Company, as this does not constitute "communication" in the technical sense. The Data Controller identifies the subjects of the company's staff authorized to receive data from the Data Processor. On the other hand, any external data transmission must be expressly and previously authorized by the Data Controller;
8. the processing of personal data for unauthorised purposes unrelated to the work of the Person in charge is strictly prohibited. It is strictly forbidden to use the tools provided by the Data Controller (hardware, software, etc.) for unauthorized purposes, unrelated to the work of the Data Processor. It is strictly forbidden to reproduce the documents available to the Data Controller for purposes unrelated to its duties;
9. it is strictly forbidden to communicate to third parties the access credentials to the hardware and software systems, as well as to the accounts provided to the Data Subject by the Data Controller. It is strictly forbidden to duplicate access keys to the premises, cabinets where documents containing personal data are kept and archived. Upon termination of his/her duties, the Person in Charge returns logical and physical keys of access to the Data Controller's archives;
10. the Person in Charge shall promptly report to the Data Controller any behaviour and any fact that may constitute a personal data breach, as well as any malfunctioning of the IT systems used by the Company. In particular, it reports the date of detection of the risk, the location of the risk, the description of the risk and any other information useful for preventing unlawful processing, a breach of personal data, as well as limiting its harmful consequences;

11. the Person in charge will retain his or her position until any revocation, or until the end of the collaboration or employment relationship;
12. this assignment does not entail any salary and contractual changes to the current employment relationship as they are exclusively aimed at the application of the Regulation on the processing of personal data;
13. in carrying out his or her duties, the Person in Charge is authorised:
    a. to process any data necessary for the performance of their work. It must comply with the limits set out in the policy referred to in point 6, as well as any other directive issued by the Data Controller in compliance with the Regulation and applicable legislation;
    b. to be assisted by other employees of the company, with purely material tasks, coordinating their activities and giving them instructions and/or transmitting to them those issued by the Data Controller;
14. improper processing and use pursuant to points 8 and 9 above, as well as other violations of this assignment constitute a serious disciplinary offence. They also constitute just cause for dismissal and/or cause for termination of the employment contract between the Data Controller and the Data Subject, without prejudice to the Data Controller's right to compensation for the damage caused.

[DD/MM/YYYY], Milano

The Data Controller : _____

For receipt and acceptance of the assignment by the Data Processor M-CUBE SPA: _____



ANNEX 2: APPOINTMENT AS AN EXTERNAL PERSON IN CHARGE OF THE PROCESSING OF M-CUBE'S PERSONAL DATA

The undersigned Manlio Romanelli, in his capacity as legal representative of **"MCUBE SPA",** with registered office in via San Galdino n.6, 20154, Milan, Registration Number in the Milan Business Register and Tax Code no.01022540320- Tel: 040634364, E-mail: info@mcubedigital.com; PEC: mcube@pec.it - Data Controller pursuant to EU Regulation 2016/679,

NOMINATION

The person in charge of the processing of personal data is [Mr./Mrs Name Surname], born in [City, Province or Region, State], in date [DD/MM/YYYY] having address at the working site of [NAME OF THIRD PARTY COMPANY] in [address]. In order to correctly apply EU Regulation 2016/679 (hereinafter also referred to as the "Regulation") and to adequately protect the rights of the Data Subjects, the following operations will be carried out:
- ensure and ensure that all customers and suppliers falling within the scope of the GDPR have signed the consent to the processing of data and have received the information on the processing of data;
- ensure and ensure that all external Managers have signed the appointment in relation to their specific tasks and for the authorized purposes;
- take care of the updating of the List of External Managers;
- support the subsidiaries (branches) in the adoption and implementation of the Group Privacy Policy, also by making use of external professionals;
- analyze whether there are new processes that may lead to a change in risk in data processing;
- communicate the results of the aforementioned analysis to the Group's "Compliance" organisational function (privacy@mcubedigital.com);
- immediately notify the Group's "Compliance" (privacy@mcubedigital.com) organisational function of any data breaches and provide immediate support in the management of these cases.

With this act of appointment, in compliance with the provisions of the Regulations, it is provided that:

1. all the data of which the Person in Charge becomes aware by reason of his role, task, company function, are processed by the Person in charge exclusively for the performance of his or her work on behalf of the Data Controller, for the time strictly necessary;
2. it is not permitted to communicate such data to third parties, unless the communication is essential for the performance of the work of the Person in Charge and takes place towards third parties authorised by the Data Controller, in the manner provided by the latter;
3. the Person in charge processes personal data in compliance with the principles of lawfulness, fairness, transparency, only for the purposes for which such data were collected (so-called purpose limitation) and only to the extent necessary for the pursuit of these purposes (so-called processing minimization);
4. the personal data processed must be accurate and, if necessary, updated and stored for the time strictly necessary to pursue the above purposes (so-called storage limitation);
5. the Data Processor processes the data following the instructions given by the Data Controller in order to ensure adequate security of the personal data processed, as well as respect for the rights and freedoms of the data subjects;
6. the Data Controller informs the Data Processor of the privacy policies adopted, which are always available to the Data Processor for consultation. Please refer to the policy document for any instructions to be followed in the processing of personal data;
7. the Person in Charge is authorised to transmit data within the Company, as this does not constitute "communication" in the technical sense. The Data Controller identifies the subjects of the company's staff authorized to receive data from the Data Processor. On the other hand, any external data transmission must be expressly and previously authorized by the Data Controller;
8. the processing of personal data for unauthorised purposes unrelated to the work of the Person in charge is strictly prohibited. It is strictly forbidden to use the tools provided by the Data Controller (hardware, software, etc.) for unauthorized purposes, unrelated to the work of the Data Processor. It is strictly forbidden to reproduce the documents available to the Data Controller for purposes unrelated to its duties;
9. it is strictly forbidden to communicate to third parties the access credentials to the hardware and software systems, as well as to the accounts provided to the Data Subject by the Data Controller. It is strictly forbidden to duplicate access keys to the premises, cabinets where documents containing personal data are kept and archived. Upon termination of his/her duties, the Person in Charge returns logical and physical keys of access to the Data Controller's archives;
10. the Person in Charge shall promptly report to the Data Controller any behaviour and any fact that may constitute a personal data breach, as well as any malfunctioning of the IT systems used by the Company. In particular, it reports the date of detection of the risk, the location of the risk, the description of the risk and any other information useful for preventing unlawful processing, a breach of personal data, as well as limiting its harmful consequences;
11. the Person in charge will retain his or her position until any revocation, or until the end of the collaboration or employment relationship;
12. this assignment does not entail any salary and contractual changes to the current employment relationship as they are exclusively aimed at the application

of the Regulation on the processing of personal data;

13. in carrying out his or her duties, the Person in Charge is authorised:
    a. to process any data necessary for the performance of their work. It must comply with the limits set out in the policy referred to in point 6, as well as any other directive issued by the Data Controller in compliance with the Regulation and applicable legislation;
    b. to be assisted by other employees of the company, with purely material tasks, coordinating their activities and giving them instructions and/or transmitting to them those issued by the Data Controller;
14. improper processing and use pursuant to points 8 and 9 above, as well as other violations of this assignment constitute a serious disciplinary offence. They also constitute just cause for dismissal and/or cause for termination of the employment contract between the Data Controller and the Data Subject, without prejudice to the Data Controller's right to compensation for the damage caused.

11/12/2023, Milano

The Data Controller: 

For receipt and acceptance of the assignment by the Data Processor:

[Name Surname] _____