






**POLICY REGARDING THE PROCESSING OF PERSONAL DATA OF EMPLOYEES, INTERNS AND COLLABORATORS
PURSUANT TO ARTICLES 13 AND 14 OF EU REGULATION 2016/679 ("GDPR")
AND NATIONAL LEGISLATION ON PRIVACY**

	DATA PROCESSING CONTROLLER	Fondazione MAIRE – Ente del Terzo Settore ("Foundation" or "Data controller") Piazzale Flaminio, 9 – 00196 Rome, Italy Tax ID.: 96477180580 T.: +39 06 4122 35303 PEC: fondazionemairetecnimont@pec.it E-mail : secretary@fondazionemaire.com
---	-----------------------------------	---


	PERSONAL DATA PROCESSED (COMMON DATA) Identification, administrative and professional information, such as in the following non-exhaustive details: <ul style="list-style-type: none"> - Name, surname, gender, place and date of birth, marital status and nationality, home address and/or domicile address, telephone contact numbers and personal emails, identification document details (identification card and/or passport) and, where applicable, residency and work permits, tax identification number or equivalent national identification code, family members and their identification details; - current account details (IBAN), social security, insurance and tax details and, where applicable, the relative services and/or obligations; - Data contained in the CV, education and professional experience and skills acquired and memberships in any rolls/register and professional associations; - voice messages, emails and any work document created, archived and/or transmitted using company instruments such as personal computers, tablets, smartphones, etc.; - information acquired through the company security systems, including the access and TVCC systems.
---	---

	PARTICULAR CATEGORIES OF PERSONAL DATA PROCESSED (SENSITIVE DATA) Information regarding health, membership in labour and/or political associations, religious faith such as, as a non-exhaustive example: <ul style="list-style-type: none"> - workers' health certification, certification of membership in the so-called "Protected categories", illness, accident and maternity certificates and in general information regarding absences due to illness and for usage of health treatments and/or paid leave; - information regarding offices held in unions and/or political offices and/or administrative data regarding membership in the aforementioned associations; - requests for leave due to religious holidays.
---	---


	SOURCE OF DATA AND CATEGORIES OF DATA COLLECTED AT THIRD PARTIES The data is collected from the interested party (therefore it is provided directly by you), or it is acquired from third parties (as a non-exhaustive example: from the various tax, social security, insurance authorities and authorised professionals, whether European or not, as well as from European and/or non-European legal entities that belong to the MAIRE group.
--	---


	PROCESSING PURPOSES			LEGAL BASIS OF PROCESSING	DATA RETENTION PERIOD
	<p>Purposes related to the establishment and management of the employment relationship, including, for example:</p> <ul style="list-style-type: none"> - administration of personnel: processing of payroll and compensation payable and fulfilment of all legal, tax, social security and insurance obligations upon hiring/ while the relation is ongoing and upon termination; - handling of the personnel, the so-called “Worker Dossiers” and publication of the relative information on the Group platform; - management of the development, training and compensation processes; - management of the organisational processes; - management of processes which relate to international mobility of personnel pursuant to the applicable laws in the interested party’s country of destination or nationality; - management of the company equipment assignment processes. 	<p>Execution of the employment contract and, as regards the particular categories of data, fulfilment of the obligations and exercise of the rights of the controller or parties concerned in the field of labour law and social security and social protection insofar as it is authorized by the Law of the EU or Member States or a collective contract under the law of Member States, in the presence of appropriate guarantees for the fundamental rights and interests of parties concerned.</p>		<p>Contractual duration and, after termination, for a period of 10 years, except for the paper folder of the employee, which will be stored for 20 years.</p>	
	<p>Fulfilment of obligations or exercise of rights under national or European Union law or collective contracts in accordance with national law. In particular, for the following purposes:</p> <ul style="list-style-type: none"> - management of administrative-accounting obligations; - industrial relations management; - management of health and safety at work. 	<p>Need to comply with the legal obligations to which the data controller is subject, and with regard to the particular categories of data, fulfill the obligations and exercise the rights of the controller or parties concerned in the field of labor law and social security and social protection in accordance with the provisions of art. 9.2, lett. b) GDPR or for purposes of preventive medicine or occupational medicine, assessment of the employee's ability to work by the competent doctor pursuant to article 9, paragraph 2, letter h) and in compliance with the provisions of article 9, paragraph 3 of the GDPR.</p>		<p>Contractual duration and, after termination, for the period of 10 years.</p>	
	<p>Purposes related:</p> <ul style="list-style-type: none"> - to the management of internal controls, as well as of internal or external control bodies, such as board of statutory auditors, independent auditors, certification entities. 	<p>Legitimate interest (Protection of the company and of the corporate assets. Safety).</p>		<p>Until the end of the employment relationship and, after termination, for the period of 10 years.</p>	
	<p>If necessary, to ascertain, exercise or defend the rights of the Controller in court, including the management of labour law disputes;</p>	<p>Legitimate interest (defence in court).</p>		<p>In the case of judicial litigation, for the entire duration of the same, until the exhaustion of the terms of practicability of appeals.</p>	

Control of physical access (including video surveillance) in order to guarantee the security of people and goods (in compliance with article 4 of the Workers' Statute and subsequent amendments, the equipment installed is not designed for remote control of work activity).	Legitimate interest (Protection of the company and corporate assets. Security).	Video surveillance: 24 hours from the moment the images were detected.
		Physical access control, different from video surveillance 10 years from the moment physical access was detected
Control of logical access to company information systems, in order to guarantee the security of people and goods (ex. log management, system administrator log management, digital identity).	Legitimate interest (Protection of the company and corporate assets. Security)	1 year from the moment logical access was detected 6 months for system administrator access logs
Publication also of the CV and/or photo on the company Intranet portal	Legitimate interest (better management of the internal company organization)	For the entire contract duration.
Once the above retention terms have elapsed, the data will be destroyed, deleted or made anonymous, consistent with the technical procedures for deletion and backup.		

	DATA SUPPLY
	Obligatory for the stipulation or complete execution of the employment and/or collaboration contract and to fulfil legal obligations. The refusal to supply data shall not allow the establishment or continuation of the employment and/or collaboration relationship.

	CATEGORIES OF DATA RECIPIENTS
	The data may be communicated to parties operating as data controllers , including, in particular, tax, social security, insurance authorities, qualified professionals, companies for administrative-accounting purposes, banks and credit institutions, auditing firms, supervisory and control authorities and bodies and in general public or private parties entitled to request data. Moreover, data can be communicated to European and non-European companies of the Maire Tecnimont Gro MAIRE group up as well as, for contractual and commercial purposes, to clients, suppliers and partners.
	The data may be processed, on behalf of the controller, by parties also belonging to the MAIRE group and designated as external data processors , including, in particular, companies responsible for managing the personnel administration processes, the development, training and compensation processes, organizational processes, processes related to personnel international mobility, IT, security and surveillance services.

	PARTIES AUTHORIZED FOR PROCESSING
	The Data may be processed by employees and collaborators of the Foundation belonging to departments responsible for the pursuit of the aforementioned purposes that have been expressly authorized for processing and have received adequate operating instructions.

	TRANSFER OF PERSONAL DATA IN COUNTRIES NOT BELONGING TO THE EUROPEAN UNION
	The Data may be transferred to non-European countries to legal entities belonging to the MAIRE group or to other subjects by virtue of a contractual or commercial relationship or for specific business requirements. Transfers are occasional and necessary for the execution of the employment and/or collaboration contract with parties concerned or in order to terminate or execute a contract between the company or other natural or legal persons in favour of the party concerned, and therefore admitted pursuant to article 49.1, letter b) and c) of the GDPR.



RIGHTS OF PARTIES CONCERNED - COMPLAINTS TO THE CONTROL AUTHORITY

By contacting the Group Corporate Affairs Department, Governance, Ethics & Compliance Depart. via e-mail privacy@groupmaire.com parties concerned may:

- ask the data controller to have access to their data, the correction, integration or deletion thereof, as well as the limitation of processing;
- oppose processing in the hypotheses of legitimate interest of the controller¹;
- receive the data in a structured form that is commonly used and legible by an automatic device, and, if technically feasible, transmission thereof to another controller without impediments ("right to data portability")².

Parties concerned shall also have the right to file a complaint with the competent Supervisory Authority.

¹ The right to limit processing consists of temporarily subjecting the data preservation, in the following cases pursuant to art. 18 of the GDPR:

- a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

² The right to data portability can be exercised if the processing is based on consent or a contract and it is carried out using automated instruments.