









**PRIVACY NOTICE ON THE PROCESSING OF SUPPLIERS' PERSONAL DATA**

Pursuant to Articles 13 and 14 of the EU Reg. no. 679/2016 ("GDPR"), this privacy notice explains how and for what purposes Microelettrica Scientifica S.p.A. processes the personal data of its actual or potential suppliers ("Suppliers").

<p><b>1. DATA CONTROLLER</b></p> 	<p>The Data Controller is <b>Microelettrica Scientifica S.p.A.</b>, with registered office in (20090) Buccinasco (MI), Via Lucania, 2/4/6; Email: <a href="mailto:privacy@microelettrica.com">privacy@microelettrica.com</a> ("Microelettrica" or "Data Controller").</p> <p>Please note that, in some cases, other affiliated companies of the Knorr-Bremse Group, as well as the parent company Knorr-Bremse AG, may have access to Personal Data, as defined below, acting as Data Controllers or Joint Controllers of Microelettrica ("Knorr-Bremse Group"). The contact data of all Knorr-Bremse companies can be found at: <a href="https://www.knorr-bremse.com/en/company/knorr-bremse-worldwide/">https://www.knorr-bremse.com/en/company/knorr-bremse-worldwide/</a>.</p>
<p><b>2. DATA SUBJECTS AND TYPES OF PERSONAL DATA ACQUIRED</b></p> 	<p>Microelettrica may process Personal Data of legal representatives and/or contact persons of Suppliers, with whom Microelettrica has a business relationship and/or a discussion/negotiation is underway for the establishment of a business relationship.</p> <p>In this context, the following types of personal data may be processed:</p> <ul style="list-style-type: none"> <li>a) <b>personal and contact data</b> such as, for example, name and surname, date and place of birth, tax code, work telephone numbers (fixed and/or mobile) and e-mail addresses of contact persons;</li> <li>b) <b>corporate data</b> such as VAT number, physical and telematic address, telephone numbers, as well as the name and surname, place, date of birth and tax code of the legal representative(s) or other persons with powers of representation, and commercial data such as VAT number, tax code, date and place of birth, physical and telematic address, telephone numbers (fixed and/or mobile) in the case of a Supplier-individual;</li> <li>c) <b>payment data</b> such as account number/IBAN; (for data under (a) to (c): "Common Data")</li> <li>d) <b>computer data</b> (access logs, IP address, etc.) derived from the activities carried out for the Data Controller (e.g. for the management of platforms, applications and/or HW and SW infrastructures pertaining to the Data Controller, also for the maintenance activities of the same) and/or from the use of platforms pertaining to the Data Controller to which the Suppliers are enabled ("Computer Data");</li> <li>e) <b>data on criminal convictions/offences</b> ('Judicial Data');</li> <li>f) <b>any further information acquired in the course of the business relationship, as well as during discussions/negotiations functional to the establishment of a business relationship</b> (by way of example but not limited to qualifications and/or certifications of employees, as better indicated under point h), below), <b>or provided voluntarily by the Supplier and relating to his professional and/or business activities</b>, where such information is relevant to the identification, even indirectly, of natural persons;</li> <li>g) <b>personal data</b> collected from public sources, such as integrity/reliability and creditworthiness databases, credit agencies and third-party companies specialized in providing this data (info providers), including any additional publicly available information, e.g. through excerpts from chamber of commerce reports, press reports, financial information and information on relevant and significant litigation or other legal proceedings in which the Supplier may be involved.</li> <li>h) <b>personal data relating to the Supplier's employees</b>, acquired in the performance of a project contract, such as, but not limited to, data from pay slips and relating, for example, to health benefits or labor union memberships and/or other documentation necessary for the performance of the contractual relationship in place with the Supplier (e.g. UNILAV, LUL, health eligibility, etc.) ('Special Data').</li> </ul> <p>(Common Data, Computer Data, Judicial Data, additional information <i>under</i> (f) and (g) and Special Data above will be jointly referred to as 'Personal Data')</p>
<p><b>3. PURPOSE OF PROCESSING</b></p> 	<p>Personal Data are processed for the following purposes:</p> <ul style="list-style-type: none"> <li>a) <b>execution of pre-contractual measures</b> prior to the establishment of a business relationship and/or the maintenance of the same upon renewal and/or modification of an existing business relationship;</li> <li>b) <b>execution of the contract</b> and, more generally, of the commercial relationship with Microelettrica and related management of the existing contractual/commercial relationship (e.g. to execute agreements, to provide instructions, for related service communications and/or to process payments, for the management and settlement of contractual and conventional guarantees, as well as for the fulfilment of any other obligation arising from the contract, such as, registration and archiving of personal data);</li> </ul>

	<ul style="list-style-type: none"> <li>c) <b>legally required fulfilments in the field of taxation and accounting and</b> related administrative-accounting, auditing, invoicing and collection activities;</li> <li>d) <b>fulfilment of legal obligations</b>, such as those concerning the fight against money laundering and the financing of terrorism and safety at work, as well as monitoring the Supplier's compliance with company procedures and industry practices;</li> <li>e) <b>IT security</b> pursued through the control and monitoring of the systems pertaining to the Data Controller, which may also be made available to the Supplier for the performance of the activities entrusted to it (access to websites, web apps, reserved environments, e-mail boxes, systems administration, etc.);</li> <li>f) <b>prevention of abuse and/or security threats, fraud or other criminal or malicious activities</b> to ensure the security of the services provided, including possibly via the web, and for the security and capability of a network or servers connected to it to withstand, at a given level of security, unforeseen events or unlawful or malicious acts that compromise the availability, integrity and confidentiality of personal data stored or transmitted;</li> <li>g) <b>management of any litigation</b>, for the purpose of protecting and/or exercising the right of defence of the Controller, in the context of dispute resolution, enforcement of contractual agreements and/or in the context of litigation.</li> </ul>
<b>4. LEGAL BASIS OF PROCESSING AND NATURE OF CONFERMENT</b>	
	<p>The processing of Personal Data is carried out in accordance with the following legal bases:</p> <ul style="list-style-type: none"> <li>a) <b>performance of pre-contractual and/or contractual measures</b> (Art. 6, c. 1, lett. b), GDPR) at every stage of the business relationship (from negotiation, to execution, to termination), with regard to the <u>purposes set out in letters a) and b) of Art. 3, above;</u>  <i>The <u>provision of Personal Data is mandatory</u>. This means that, in the absence of such provision, the contractual/commercial relationship will not be possible.</i></li> <li>b) <b>fulfilment of legal obligations</b> (Art. 6, c. 1, lett. c), GDPR), with regard to the <u>purposes set out in letters c) and d) of Art. 3, above.</u>            If, in the context of the purpose referred to in letter d) of Article 3, the processing relates to Special Data, such processing will be carried out in order to fulfil the obligations and exercise the specific rights of the Data Controller or the data subject in the field of employment, social security and social protection law (Art.9 par.2, letter b), GDPR).  <i>The <u>provision of Personal Data is mandatory</u>, as it is necessary for the Data Controller to fulfil its legal obligations related to the management of the existing business relationship between the parties. Failing this, the Data Controller will not be able to continue the existing relationship.</i></li> <li>c) <b>legitimate interest of the Data Controller</b> (Art. 6, c. 1, lett. f), GDPR), with regard to the <u>purposes set out in sub-paragraphs e), f) and g) of Art. 3, above</u> (in this context, data from public sources may also be used for integrity/solidity/reliability checks);  <i>Although the <u>provision of Personal Data is not mandatory</u>, it is in any case necessary because such data is strictly connected and instrumental to the pursuit of the legitimate interest of the Data Controller, there being a fair balance between the latter and the interests, rights and freedoms of the data subject, and any refusal to provide Personal Data may make it impossible to provide the services requested.</i>            Legitimate interest also constitutes the legal basis for the processing of Computer Data.</li> </ul>
<b>5. COMMUNICATION OF PERSONAL DATA AND EXTRA-EU TRANSFERS</b>	
	<p>Personal Data are processed in connection with the contract and the obligations, including legal and/or regulatory obligations, arising therefrom.</p> <p>Personal Data shall not be disclosed, but may be communicated to subjects acting on behalf of the Data Controller such as, for example, (i) subjects authorised by Microelettrica (e.g. employees and/or collaborators); (ii) freelancers and law firms/consulting companies in compliance with legal obligations and/or in execution of administrative-judicial measures or if necessary for the assertion, exercise or defence of the Data Controller's rights; (iii) banks, financial and insurance institutions, credit institutions; (iv) companies that manage IT networks and systems and/or suppliers of IT maintenance services; (v) auditors; (vi) subjects with control functions.</p> <p>Data may also be disclosed for administrative-accounting purposes to companies belonging to the Knorr-Bremse Group with which special agreements exist due to the shared processing purposes and the provision of services pertaining to the current business activities of the Data Controller.</p> <p>Personal Data will not be communicated and/or transferred to third countries outside the EU. Should this be necessary, again for the performance of obligations arising from the contract, transmission will take place in full compliance with Articles 44 et seq. of EU Regulation 679/2016.</p>

<b>6. PROCESSING METHOD</b>	
	<p>Personal Data may be processed in both electronic and paper format, and Personal Data will be collected and processed both at the Data Controller's premises and, where applicable, at the premises of the recipients mentioned above.</p> <p>Personal Data will be processed by specially authorised and trained internal persons. These are granted access to Personal Data to the extent and within the limits necessary for the performance of the processing activities concerning the data subject. Judicial Data and Special Data will be processed by means of technical and organisational security measures suitable to guarantee its protection and confidentiality.</p>
<b>7. RETENTION PERIOD</b>	
	<p>The Personal Data (excluding Computer Data) processed by the Data Controller are kept for the time necessary to carry out the activities related to the management of the contract with the Data Controller and up to ten years after its conclusion (art. 2946 of the Italian Civil Code.) or from when the rights that depend on it can be asserted (pursuant to Article 2935 of the Italian Civil Code); as well as for the fulfilment of obligations (e.g. tax and accounting obligations) that remain even after the conclusion of the contract (Article 2220 of the Italian Civil Code), for which purposes the Data Controller must only retain the data necessary for their pursuit. This is without prejudice to cases in which the rights deriving from the contract have to be asserted in court, in which case the data, only those necessary for such purposes, will be processed for the time necessary for their pursuit.</p> <p>For Computer Data, the duration of retention depends on the risk alleged and/or detected and the prejudicial consequences thereof, without prejudice to measures to render the data anonymous or to limit its processing. In any case, the data must be retained (starting from the knowledge/detection of the danger event or data breach) for the time necessary to notify the Supervisory Authority of the data breach detected through the procedures implemented by the Data Controller and in any case to remedy it.</p>
<b>8. RIGHTS OF THE DATA SUBJECT</b>	
	<p>Pursuant to Art. 15 et seq. of the GDPR, data subjects may, at any time and to the extent applicable to the case at hand, exercise the following rights: <b>(i) the right of access</b> to Personal Data; <b>(ii) the right to rectification</b> of inaccurate or incomplete data; <b>(iii) the right to erasure</b> of Personal Data; <b>(iv) the right to restriction of processing</b> of Personal Data; <b>(v) the right to receive</b> Personal Data in a structured, commonly used and readable format and the right to have such data transmitted to another Data Controller (<b>right to portability</b>).</p> <p>In the case of processing based on legitimate interest and where there are grounds based on the particular situation of the data subject, the data subject shall also have <b>(vi) the right to object</b> to the processing of Personal Data.</p> <p>In any case, the data subject always has <b>(viii) the right to lodge a complaint</b> directly with a supervisory authority which, for Italy, is the <i>Italian Data Protection Authority - Garante per la protezione dei dati personali</i> (see <a href="http://www.garanteprivacy.it">www.garanteprivacy.it</a>), or the right to appeal to the competent judicial authority.</p>

Last updated: June 2024