INFORMATION ON PERSONAL DATA PROCESSING FOR ACCESS TO CONFIDENTIAL AND SECURE COMMUNICATION TOOL

- Pursuant to Article 13 of the Regulation 679/2016/EU on personal data protection -

Dear Supplier/Customer,

Corporate information, whether in paper or electronic form, is increasingly to be considered a strategic asset of any company, which must be guaranteed adequate level of protection, whether it relates to the company itself or to third parties (Suppliers/Customers).

Brembo, in the context of its corporate policies on information security, has therefore decided to pursue the following objectives:

- The company's know-how protection, with focus to all information stored in the information system;
- Protection of Customers and Suppliers' data, also as required by them;
- Supporting the increasingly pervasive digitalization of business processes with an infrastructure that is consistently secure and aligned with market best practices.

Among the tools adopted for good governance of information systems management, to assure an adequate level of protection of corporate information, Brembo has decided to implement the Microsoft Information Protection ("**MIP**") tool.

Therefore, should it become necessary to share confidential information and documents with you in the context of your relationship with Brembo, in order to do so in a secure manner, you may be given access to the MIP system used by Brembo.

As accessing this tool involves collecting and processing certain personal data of users who access to the documentation through the recognition of the related account, Brembo N.V. (hereinafter "**Brembo**" or the "**Company**"), in its role of data controller, wishes to provide you with the following information pursuant to Article 13 of European Regulation 679/2016 on personal data protection ("**Regulation**")[1].

It should be noted that, in the event of Brembo information being shared through MIP, the only relevant information regarding the processing of personal data by the Company are exclusively those listed below, being excluded any further and/or different processing possibly represented by third parties during verification and recognition of the authorized account.

1. Types of personal data

The data of the users authorized by You to the access at the documentation that may be shares through the MIP system (thereinafter "**Data Subjects**") for the sharing of information in a secure and confidential manner within the context of the execution of agreements with the Company, including name, surname, e-mail address, IP address, location and technical data of use of the application, also related to the device used if needed, will be processed by the Company in accordance with the relevant regulations on personal data protection.

2. Purpose of processing

Data Subjects' personal data processing is done by the Company in order to ensure the secure and confidential sharing of documents, within the context of the management and execution of the contractual relationship (including the management of the pre-contractual relationship). For the aforementioned purpose, it is not necessary to obtain consent as the processing is based on the Company's legitimate interests in protecting its information and business assets (pursuant to Art. 6.1 f) of the Regulation).

[1] EU Regulation no. 2016/679 on personal data protection came into force in 2016 and it is applicable in all Member States since May 25th 2018.

3. Nature of collection and processing methods

The collection of personal data concerning a Data Subject is necessary and, without it, it will not be possible to share with the Company confidential documentation and information and to fulfil the obligations and commitments arising from the business relationship.

The data shall be processed by the Company and its authorized personnel and in particular by the personnel of the Company's department which is your main interlocutor within the Company, and by the staff of the Information & Communication Technologies Department, to ensure the functioning of the secure communication system and the resolution of any anomalies, in accordance with the principles of correctness, lawfulness and transparency provided for by the applicable legislation on personal data protection, protecting the confidentiality of Data Subjects by adopting technical and organizational security measures designed to ensure an adequate level of security (for example: preventing the access by unauthorized persons, or restoring access to data in the event of physical of technical incident).

4. Disclosure, dissemination and transfer of data

The Company uses third parties for the provision of services that involve the processing of personal data, including, for example purposes, suppliers of technological services to support the protection of documents exchanged. These entities work as data processors, on the basis of specific and appropriate instructions in terms of processing procedures and security measures indicated in the relevant contractual documentation. In particular, the abovementioned personal data will also be processed on our behalf by Microsoft as data processor, within the limits of the provision of the services. The complete and up-to-date list of subjects who process personal data as data processors is available on request at the Company, at the contacts indicated below.

The data may be disseminated to other Group companies, including subsidiaries both located in the European Union and outside the European Union (whose updated list is available on the institutional site of Brembo), where necessary in the event that they are required to cooperate in the performance of contractual obligations. Similarly, in relation to the MIP service, Microsoft may transfer personal data outside of the European Union, including to the United States. In this case, with respect to transfers outside the European Union, the Company undertakes to ensure adequate levels of protection and safeguards, also contractual, including appropriate technical and organizational measures, according to the applicable rules, including the stipulation of standard contractual clauses (you can request a copy of the commitments made with the Group Companies in the context of these clauses by sending a request to the Company at the contacts indicated below). Personal data will not be disclosed.

5. Data retention and processing of account data by third parties

The data will be stored in accordance with applicable data protection regulations for the time that is necessary to fulfil the above-mentioned purposes. In particular, data such as IP address, location and technical usage data will be stored for 30 days.

It should be noted that data such as name, surname and email address will be retained even after the end of your contractual relationship with the Company, by both the Company and Microsoft, as data controller, since this is an account that will be created by you directly on Microsoft platform and in accordance with Microsoft privacy policy, which we invite you to read.

6. Rights of Data Subjects

A Data Subject shall have the rights contemplated in the Regulation (articles from 15-21) in respect of the processing of data contemplated thereto, including the right to:

- Obtain confirmation of the existence of personal data concerning him/her and to gain access to them (right of access);
- Obtain the updating, modification and/or rectification of its personal data (right of rectification);

- Obtain erasure, or to set limits to processing, of personal data whose processing is unlawful, including those that are no longer necessary in relation to the purposes for which they were collected or otherwise processed (right to be forgotten and right to the restriction of processing);
- Object to processing (right to object);
- Withdraw previously given consent, if any, without prejudice to the lawfulness of processing based on that consent;
- Receive a copy in electronic form of the data concerning him or her which have been provided to a controller in the framework of an agreement and to have such data transmitted to another controller (right to data portability).

For the exercise of the rights above and in case of further requests for information regarding the present privacy notice, the Data Subject can contact the Data Protection Officer (DPO) by sending an email to privacy@brembo.com or by a written communication to the legal address of the Company, to the attention of the DPO.

Data Subject may also lodge a complaint with the Supervisory Authority in case of infringement of regulations concerning the protection of personal data.

7. Identity and contact details of the Controller and contact of the Data Protection Officer

The Data Controller is Brembo N.V., with legal seat in Amsterdam, the Netherlands, and with business and corporate address in Bergamo, via Stezzano 87 – 24126, Italy, phone number 035.6052111, represented by its Legal Representative for the time being.

The Data Protection Officer (DPO) is available at the following e-mail address privacy@brembo.com