Annexure no to the Service Agreement

DATA PROCESSING AGREEMENT

Concluded by and between:

, a company incorporated under the laws of , having its registered office and principal place of business at , and registered with the under number (hereinafter to be referred to as: the "**Controller**"),

and

, a company incorporated under the laws of , having its registered office and principal place of business at , and registered with the under number (hereinafter to be referred to as: the "**Processor**").

1. Subject matter of Data Processing Agreement and definitions

1.1. This Data Processing Agreement applies to the processing of personal data subject in the scope of the agreement of between the parties for the ("Services") (hereinafter to be referred to as: the "Service Agreement").

1.2. The terms:

"Data Protection Laws" mean any relevant international or national binding laws regulating the use and protection of Personal Data, including but not limited to the GDPR, CCPA, UK Data Protection Act 2018 (and any replacement law that may be issued by the United Kingdom in relation to the UK Brexit), as well as related guidance, instructions or opinions and judgments issued by the competent public authorities or courts of law.

"The GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"The CCPA" means Assembly Bill 375 of the California House of Representatives, an act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy and approved by the California Governor on June 28, 2018.

1.3. Any capitalized terms not otherwise defined in this Data Processing Agreement shall have the meaning given to them in the Service Agreement. Except as modified below, the terms of the Service Agreement shall remain in full force and effect. Other terms used in this Data Processing Agreement shall have meanings ascribed to them in GDPR, including but not limited to "processing", "personal data", "controller", "processor" and "data subject", unless it is otherwise provided in this Data Processing Agreement.

2. Processing instructions

2.1. The Processor shall process the Personal Data only on documented instructions from the Controller, including any transfer of data to third countries or international organizations. The Controller's instructions are included in the Appendix 1 hereto and in the Service Agreement and may be updated from time to time when requested by the Controller - amongst others - due to changes to the Service Agreement or if so required under applicable Data Protection Laws.

2.2. The Processor guarantees that it has appropriate technical and organizational measures in place to meet the requirements of the Data Protection Laws and that it will ensure protection of the rights of the data subjects.

2.3. The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the Data Protection Laws.

3. Engaging Sub-Processors

3.1. The Processor may engage a third party for processing of personal data under this Data Processing Agreement (hereinafter the "**Sub-Processor**"), provided that:

(a) the Processor has notified the Controller in writing of such Sub-Processor, including any intended changes concerning the addition or replacement of such Sub-Processors, and

(b) the Controller has not objected thereto within 30 days of notification.

3.2. If the Controller does not object, the Sub-Processor is considered approved by the Controller.

3.3. The Processor shall maintain and update (as necessary) a list of all Sub-Processors used for processing of personal data on behalf of the Controller. Approved Sub-Processors as of execution of this Agreement are detailed in the instructions set forth in the Appendix 1 hereto.

3.4. The Processor shall enter into a written agreement with every approved Sub-Processor, under which the Sub-Processor undertakes obligations corresponding to those undertaken by the Processor under this Data Processing Agreement. The Processor shall always remain liable for its Sub-Processor's performance and obligations as for its own.

3.5. Where the Processor engages a Sub-Processor in a country outside the EU/EEA without an adequate level of protection, the Controller hereby authorizes the Processor to sign the EU Model Clauses with the Sub-Processor in the name and on behalf of the Controller in respect of such transfer of personal data to a third country, unless there is another specific statutory mechanism to normalize international data transfers as provided by the Data Protection Laws and specifically the GDPR.

3.6. If the Controller objects to a new Sub-Processor in accordance with the above, the Processor may not engage such Sub-Processor for processing of any personal data on behalf of the Controller. The Controller will not unreasonably object to any addition or replacement of a Sub-Processor.

4. Access Restriction, Confidentiality and Security

4.1. The Processor shall:

(a) restrict the access to Personal Data only to those of its personnel and sub-contractors for whom the access is necessary in order to properly render the Services and fulfil Controller's instructions,

(b) ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and were properly informed about the confidentiality of personal data.

4.2. The Processor shall implement appropriate technical and organizational measures in accordance with the Data Protection Laws and specifically with the article 32 of the GDPR to ensure a level of security appropriate to the risk associated with processing based on this Data Processing Agreement. These measures shall include, at a minimum, the security measures agreed upon by the parties in Appendix 1 hereto.

5. Data Subjects Requests

5.1. The Controller is obliged to facilitate the exercise of certain rights granted to data subjects in relation to processing of their personal data as provided in the Data Protection Laws and specifically in the Articles 15 to 22 of the GDPR: information and access to personal data, rectification and erasure, restriction of processing, data portability, and right to object.

5.2. The Processor, in connection with processing set out in this Data Processing Agreement, shall assist the Controller by appropriate technical and organizational measures, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights as provided by the Data Protection Laws and specifically those laid down in Chapter III of the GDPR.

6. Personal Data Breaches, Data Protection Impact Assessments and Prior Consultations

6.1. As it is provided in the Data Protection Laws and specifically in the Articles 32 to 36 of the GDPR, the Controller has certain obligations related to: notification of data breach to the supervisory authority, communication of data breach to the data subject, performing a data protection impact assessment and prior consultation with the supervisory authority in certain situations.

6.2. The Processor shall notify the Controller of a data breach without undue delay after becoming aware of it

together with providing the relevant information about the breach as required by the Data Protection Laws And specifically the GDPR, and shall further assist the Controller in ensuring compliance with the Data Protection Laws and specifically the Articles 32 to 36 of the GDPR.

7. Return and Deletion of Personal Data

The Processor shall, at the choice of the Controller, delete or return all the personal data to the Controller at the end of the provision of Services relating to processing, and delete any existing copies unless any applicable law requires storage of the personal data, not later than within 30 days after receiving the respective instruction from the Controller.

8. Audit and Compliance

8.1. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in the Data Protection Laws and specifically in the Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. The mandated auditor shall be bound by the confidentiality obligation and shall not be the competitor of the Processor.

8.2. The Processor shall be informed by the Controller with prior 30 days' notice of any of such audit or inspection.

8.3. Audits, incl. inspections shall be carried out not more often than once a year unless such audit or inspection is related to the personal data breach, mandated by the supervisory authority or respective Data Protection Law.

9. Liability

9.1. The parties acknowledge that they each respectively are liable, accountable and responsible in their respective roles as Controller and Processor under the requirements set forth in the Data Protection Laws and specifically the GDPR, and this Agreement. The Article 82.5 GDPR shall apply for recourse claims relating to claims for compensation and/ or administrative fines.

9.2. Any limitations of liability set out in the Service Agreement shall not be applicable in relation to the processing of personal data or the parties' responsibilities as Controllers and Processors, respectively.

10. CCPA

10.1. The Controller discloses the personal data to the Processor (who is a "service provider**"** as defined in the Section 1798.140(v) CCPA) only:

(a) for the valid business purpose; and

(b) in order to enable the Processor to perform the Services described in the Service Agreement.

10.2. The Processor (service provider) shall not in any event:

(a) sell personal data;
(b) retain, use or disclose personal data for any commercial purpose other than providing the Services based on the Service Agreement; and
(c) retain, use or disclose the personal data outside of the Service Agreement concluded between the Controller and the Processor.

10.3. The Processor confirms that it understands restrictions provided in this Section 10.

10.4. All not capitalised terms used exclusively in this Section 10 shall have the meaning as defined in the CCPA.

11. Final Provisions

11.1. The Processor's compensation is being included in the Service charges set out in the Service Agreement, and therefore the Processor shall not be entitled to any additional compensation for carrying out its obligations under this Data Processing Agreement.

11.2. The governing law and dispute resolution clause set out in the Service Agreement shall also be applicable to this Data Processing Agreement.

11.3. This Data Processing Agreement has been drawn up in the same number of copies as the Service Agreement.

Signed for and on behalf of the Controller	Signed for and on behalf of the Processor
Name:	Name:
Title:	Title:
Date:	Date:

Appendix 1

1. Description of Processing

<table>
<tr><td>Categories of personal data</td><td>
<table>
<tr><th>Class</th><th>Class 1</th><th>Class 2</th><th>Class 3</th><th>Class 4</th></tr>
<tr><td>Title</td><td>Legally sensitive personal data</td><td>Other high risk personal data</td><td>General personal data</td><td>Business contact and systems access data</td></tr>
<tr><td>Categories of data</td><td>Choose applicable or if this class is not in scope please put N/A:
☐ racial or ethnic origin
☐ political opinions
☐ religious or philosophical beliefs
☐ trade-union membership
☐ genetic data
☐ biometric data
☐ health data
☐ data concerning a person's sex life or sexual orientation
☐ data relating to criminal convictions and offences</td><td>Choose applicable or if this class is not in scope please put N/A:
☐ payment cardholder data or sensitive authentication data* *(including user ID, passwords and access rights to computer systems)
☐ full banking details
☐ social security, national insurance, passport or national ID data
☐ data which would affect badly personal safety or security</td><td>Choose applicable or if this class is not in scope please put N/A:
☐ data such salary, grade, performance data
☐ data on consumers such as order history, product preference, consumer interests
☐ private data (contact details, date of birth marital status, gender, nationality, etc.)
☐ Anonymized data
☐ Pseudonymized data</td><td>Choose applicable or if this class is not in scope please put N/A:
☐ organizational management data (such as job title, job responsibilities, cost center and supervisor)
☐ location and business contact details (such as e-mail address and company phone number)
☐ user ID and access rights to computer systems</td></tr>
</table>
</td></tr>
<tr><td>Categories of data subjects</td><td>[choose applicable / add your own]
☐ Eurofins Employees
☐ Eurofins Former employees
☐ Customer's personnel
☐ Supplier's personnel
☐ Marketing prospects
☐ Job candidates
☐ Patients
☐ Creditors
☐ Members of the corporate bodies of Eurofins Legal Entities
☐ Client's customers / patients
☐ Volunteers for product testing
☐ Company's premises Visitors
☐ Website Visitors
☐ General enquirers
☐ Individual investors
☐ Beneficiaries of Eurofins CSR projects
☐ Participants in Events
☐ Debtors</td></tr>
<tr><td>Nature and purpose of the processing</td><td></td></tr>
<tr><td>Duration of processing</td><td>The processing shall continue during the term of the Service Agreement, unless otherwise instructed by the Controller.</td></tr>
</table>

Controller initials ……..…….. Supplier initials: ……..…….

2. Security Measures

The Processor shall:

1. ensure that the Personal Data can be accessed only by authorized personnel for the purposes set forth in this Data ensure that the Personal Data can be accessed only by authorized personnel on a "need to know" basis for the purposes set forth in this data processing agreement;
2. take all reasonable measures to prevent unauthorized access to the Personal Data through the use of appropriate physical and logical (passwords, but preferably Multi-Factor Authentication) entry controls, securing areas for data processing, and implementing procedures for monitoring the use of data processing facilities;
3. build in system and audit trails;
4. use secure passwords, network intrusion detection technology, encryption and authentication technology, secure logon procedures and anti-malware protection;
5. account for all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of Personal Data;
6. ensure pseudonymisation and/or encryption of Personal Data, where appropriate;
7. maintain the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
8. maintain the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
9. implement a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of Personal Data;
10. monitor compliance on an ongoing basis;
11. implement measures to identify and mitigate vulnerabilities with regard to the processing of Personal Data in systems used to provide services to the Data Controller;
12. provide employee and contractor training to ensure ongoing capabilities to carry out the security measures established in policy.

The Processor shall provide without undue delay, at the Controller's request, a description of the technical and organizational measures applied in relation to processing based on this Data Processing Agreement.

3. Third Country Transfers of Personal Data

The Processor (or any approved Sub-Processor) may only transfer the personal data to a country outside the EU/EEA if such transfer has been approved by the Controller as set forth below *[choose applicable]*:

1. Processing shall not be carried out in a country outside the EU/EEA	☐
2. Processing may be carried out in a country outside the EU/EEA	☐

Applied mechanism for personal data transfer to a country outside the EU/EEA *[choose applicable if answer 2 was selected]*

Transfer to a country with an adequate level of protection	☐
Transfer based on approved Binding Corporate Rules	☐
Standard Contractual Clauses issued by the EU Commission	☐ *[if yes, the signed copy of the Standard Contractual Clauses must be attached]*
Other	☐

4. Approved Sub-Processors

Company details	**Contact person / DPO**	**Location of the processing (country)**

Controller initials ……..…….. Supplier initials: ……..…….