Supplier Data Processing Agreement ("SDPA-P")

Version June 26, 2019

1. Scope, Order of Precedence and Term

[Insert Legal Name of Supplier]("**Supplier**") has been engaged to provide services that include the Processing of Personal Information (as defined below) of Oracle's employees, customers and/or partners ("**Services**") for Insert Legal Name of Oracle Entity and/ or its ultimate parent company ("Oracle Corporation"), and any direct and indirect subsidiaries and affiliates of Oracle Corporation in place as of the Effective Date of this Supplier Data Processing Agreement ("**SDPA-P**") as well as those that succeed to the interest thereof during the term of this SDPA-P (hereinafter referred to as "**Oracle**").

In performing the Services, Supplier agrees to comply with this SDPA-P which forms an integral part of the underlying services contract [Insert Applicable Agreement Name/Number] by and between Supplier and Oracle ("**Services Contract**"), which together with this SDPA-P, constitutes parties' "**Agreement**." Other than the addition of the changes below, the terms and conditions of the Services Contract shall remain unchanged and in full force and effect; however, this SDPA-P shall replace any prior Supplier Data Processing Agreement or EU Model Clauses between Supplier and Oracle under the Services Contract. In the event of a conflict or inconsistencies between (i) the Services Contract or any of the standards and policies referenced in this SDPA-P, and (ii) this SDPA-P, this SDPA-P prevails. Capitalized terms not otherwise defined in this SDPA-P have the meaning set out in the Services Contract or Applicable Law.

2. Data Processing

With respect to Personal Information Processed by Supplier as part of the Services, Supplier shall, and shall ensure that any person Processing Personal Information on Supplier's behalf, shall:

2.1 Process Personal Information only to deliver the Services on the documented instructions received from Oracle, in compliance with Applicable Law, and shall not Process Personal Information for any other purpose, including for its own commercial benefit, unless Supplier obtains Oracle's express prior written agreement for such Processing.

2.2 Implement and maintain appropriate technical and organizational measures designed to protect Personal Information against any misuse, accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, acquisition or access in compliance with Applicable Law, including the use of industry-recognized security standards such as ISO 27001 or similar standards where appropriate.

2.3 Comply, except as otherwise agreed to expressly by Oracle in the Agreement, with the IT, physical and environmental and Human Resources security, confidentiality, training, compliance and audit, business continuity and disaster recovery, and Security Incident and reporting requirements set out in the Oracle Supplier Information and Physical Security Standards, including any appendices referenced therein ("**OSSS**") and with the Oracle Supplier Code of Ethics and Business Conduct ("**OSCoE**"). In order to address evolving business risks, security standards and regulatory compliance requirements, Oracle may update the OSSS and/or OSCoE at its discretion. Suppliers are advised to consult the most recent versions of the OSSS and OSCoE on http://www.oracle.com/corporate/supplier/index.html.

2.4 Not permit the Processing of Personal Information by any third party (including Supplier's Affiliates) without the express prior written agreement of Oracle. In case Oracle does not consent to the involvement of the relevant third party, Supplier agrees to work in good faith with Oracle to find a solution to address any concern raised by Oracle within a reasonable period of time. If Oracle approves the involvement of the relevant third party ("**Authorized Subprocessor**"), such Authorized Subprocessor shall, prior to any such Processing, have entered into a written agreement with the Supplier at least as restrictive as this SDPA-P and the relevant data protection and security terms of the Services Contract. Such agreement shall be provided by Supplier to Oracle promptly upon request by Oracle, and Oracle may share it with its customers and/or a supervisory authority competent for Oracle or the relevant customers of Oracle ("**Competent Supervisory Authority**"). Supplier shall remain responsible for all actions by the Authorized Subprocessor with respect to the Processing of Personal Information under the Agreement and shall reasonably assess the Authorized Subprocessor's compliance with its obligations. Supplier will publish on the appropriate publicly accessible website of Supplier an overview of Authorized Subprocessor involved in the performance of the Services.

2.5 Ensure that all Personal Information created, or collected by Supplier directly from Individuals on behalf of Oracle is accurate and, where appropriate, kept up to date, and ensure that any Personal Information which is inaccurate or incomplete is erased or rectified in accordance with Oracle's instructions.

2.6 Upon request from Oracle and within a reasonable time but at the latest within the time limits prescribed by Applicable Law, access, rectify, erase, restrict and/or provide an exportable copy of Personal Information from further Processing and/or use, and confirm to Oracle that Supplier has done so.

2.7 In the event that Supplier is storing and maintaining Personal Information on behalf of Oracle (or its customers):

(a) Keep databases containing Personal Information segregated from other Supplier Personal Information using logical access restrictions;

(b) Update its records with any updated Personal Information provided by Oracle within five (5) business days from its receipt, unless the parties have agreed in writing to a shorter period;

(c) Log all access to Special Personal Information, with information identifying the user accessing (or seeking access to) such Special Personal Information, when it was accessed (date and time), and whether the access was authorized or denied; and

(d) Maintain audit trails designed to detect and respond to Security Incidents, including logging atypical events (for example, access to Personal Information by unauthorized persons). These audit trails must be maintained at least for three (3) years.

2.8 Maintain readily available information and records regarding the structure and functioning of all systems and processes that Process Personal Information under the Agreement (e.g., inventory of systems and processes). Such information shall include at least a description of (i) Supplier name and contact details, and data protection officer where applicable, (ii) the categories of Processing activities performed on behalf of Oracle, (iii) if applicable, the countries to which Transfers occur, (iv) if applicable, the identity of any Authorized Subprocessors and the Processing activities subcontracted to such Authorized Subprocessors and (v) the technical and organizational measures

designed to protect Personal Information against any misuse, accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, acquisition or access.

2.9 Regularly audit business processes and procedures that involve the Processing of Personal Information under the Agreement for compliance with the Agreement. A copy of the audit results shall be provided free of charge to Oracle upon Oracle's request.

2.10 Where the Services involve Supplier receiving or collecting Personal Information directly from Individuals on Oracle's behalf, Supplier shall:

(a) seek instructions from Oracle regarding:

1. information that must be provided by Supplier to the Individual in connection with the collection, and further Processing of the Individual's Personal Information; and
2. requests by Australian Individuals to be dealt with on an anonymous or pseudonymous basis.

(b) not collect any Personal Information from an Individual without the notice and consents as required under Applicable Law;

(c) maintain records of any notices it provides and consents it obtains as necessary for the relevant purposes and provide these to Oracle upon request; and

(d) where the Personal Information includes government-related identifiers, not adopt the government-related identifier for an Individual as Supplier's own identifier of the Individual, or use or disclose the government-related identifier unless otherwise directed by Oracle.

2.11 Unless expressly prohibited from doing so by Applicable Law, promptly notify Oracle before taking any action and act only upon Oracle's instructions concerning:

(a) Any requests for disclosure of Personal Information by law enforcement, state security bodies or other public authorities ("**Authority**");

(b) Any request by an Authority for information concerning the processing of Personal Information or other confidential information in connection with the Agreement; and

(c) Any complaints or requests received directly from an Individual concerning his/her Personal Information.

Supplier will in any case assess each request for disclosure by an Authority to establish whether it is legally valid and binding on Supplier. Any request that is not legally valid or binding on Supplier will be resisted in accordance with Applicable Law. Supplier shall in any case request the Authority to put the request received on hold for a reasonable delay in order to enable Oracle and/or its customers to contact the Competent Supervisory Authority for an opinion on the validity of the relevant disclosure. If the suspension and/or notification of the request for disclosure is prohibited, such as in case of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, Supplier will request the Authority to waive this prohibition and will document that it has made this request. In any event, Supplier will, on Oracle's request but at least on an annual basis provide to Oracle (which Oracle may further share with customer and possibly a Competent Supervisory Authority) general information on the number and type of requests for disclosure of Personal Information Processed under the Agreement and received in the preceding 12 (twelve)-month period.

Supplier shall not respond to requests or complaints received directly from an Individual, unless instructed otherwise by Oracle.

2.12 Deal promptly and appropriately with inquiries of Oracle or its customers related to Personal Information Processed under the Agreement and take any steps reasonably requested by Oracle to assist Oracle and/or its customers in complying with any notification, registration or other obligations applicable to Oracle and/or its customers under Applicable Law.

2.13 Inform Oracle promptly if Supplier:

(a) has a reason to believe that it is unable to comply with any of its obligations under the Agreement and it cannot cure this inability to comply within a reasonable time frame;

(b) becomes aware of any circumstances or change in the Applicable Law, that is likely to prevent it from fulfilling its obligations under the Agreement; or

(c) has reason to believe that that any instructions of Oracle regarding the Processing of Personal Information would violate Applicable Law.

2.14 Promptly take adequate steps to remedy any noncompliance with the Agreement and/or Applicable Law regarding the Processing of Personal Information by Supplier and any Authorized Subprocessor. Oracle will have the right to temporarily restrict or suspend the relevant Processing (or parts thereof) under the Agreement until the noncompliance is remedied. To the extent remediation is not possible or unduly delayed, Oracle may terminate the Agreement in whole or in part, without liability or compensation to Supplier being due and without prejudice to other remedies that may be available to Oracle under Applicable Law.

2.15 Execute a Business Associate agreement with Oracle if the Services involve access to protected health information ("**PHI**") as defined by the U.S. Health Insurance Portability and Accountability Act ("**HIPAA**") and implement the applicable safeguards and processes for the handling of PHI that are specified in the HIPAA Privacy and Security Rules.

2.16 Agree that Oracle may at its choice:

(i) Perform audits including on-site security audits of the facilities, systems, procedures, policies and processes used in relation to the Processing of Personal Information under the Agreement ("**Systems**") to confirm Supplier's compliance with the Agreement and Applicable Law; or

(ii) Provide to Supplier a security and privacy assessment questionnaire related to Services, which Supplier will accurately and promptly complete. Such a questionnaire may include questions seeking confirmation of compliance with the Agreement and Applicable Law. Upon request by Oracle, Supplier will also supply a copy of its most recent third party assessment, such as an ISO 27001, SSAE 18 SOC 2, ISAE 3402 or similar assessment, if Supplier has had such an assessment. If, after the original security questionnaire assessment, Oracle determines that further assessment is warranted, Oracle may request, no more than annually and with 30 (thirty) days prior written notice, an assessment with a scope to be mutually agreed related to Services provided. During such an assessment, Oracle may examine Systems related to specific Services performed, to the extent that such review does not compromise confidentiality obligations to any other clients of Supplier. Supplier

will also ensure that such audits or assessments confirm compliance by any Authorized Subprocessors obligations with the terms of the Agreement.

2.17 If relevant to the Agreement with Oracle, cooperate and assist with any inquiry or audit by relevant customers of Oracle (or a qualified independent third party auditor selected by such customer), or a Competent Supervisory Authority, and Supplier shall amend the Processing of Personal Information under the Agreement in accordance with any advice or binding decisions of a Competent Supervisory Authority issued on interpretation and application of the Agreement or Processing of Personal Information hereunder, as instructed by Oracle or the relevant customers of Oracle. Supplier shall Permit Oracle to share the data protection related terms of the Agreement and audit/assessment results (performed per Section 2.16) with Oracle Affiliates, relevant customers of Oracle, and any Competent Supervisory Authority, including the U.S. Department of Commerce for Transfers of Privacy Shield Data under Section 3 below, if applicable.

2.18 Pursuant to Applicable Law and the additional requirements set out in the OSSS, implement and maintain appropriate and documented Security Incident procedures and policies designed to (i) detect, analyze, monitor and resolve Security Incidents; and (ii) promptly but at the latest within 24 hours of any actual or suspected Security Incident involving the provision of the Services, report such Security Incidents to Oracle. Such report shall contain a detailed description of the nature of the Security Incident, categories and approximate number of Personal Information records and Individuals concerned, name and contact details of a contact point where more information can be obtained, likely consequences of the Security Incident, and measures to address the Security Incident.

2.19 At Oracle's sole discretion, return or delete Personal Information pursuant to the OSSS after the termination of the Services Contract or upon Oracle's request.

3. Transfers of Personal Information

3.1 Restricted **transfers from the EEA (including Switzerland).** This Section applies solely when the Processing of Personal Information by Supplier or its Authorized Subprocessors involves a Transfer from a Member State of the EEA, to Supplier or its Authorized Subprocessors (i) located outside the EEA and (ii) not covered by an Adequacy Decision.

(a) **Oracle as Data Controller**. Where Oracle Processes the Personal Information for its own purposes as Data Controller, the following will apply:

1. **Supplier BCR-P.** Where the Transfer to Supplier is covered by Supplier's Binding Corporate Rules for Processors, Supplier represents, warrants, and covenants (i) that it will maintain its EEA authorization of its Binding Corporate Rules for Processors for the duration of the Agreement, (ii) to promptly notify Oracle of any subsequent material changes in such authorization, and (iii) to downstream any of its obligations under its Supplier Binding Corporate Rules for Processors to Authorized Subprocessors by entering into an appropriate onward transfer agreement with any such Authorized Subprocessor.

2. **EU Model Clauses.** To the extent the Transfer is not covered by the above Transfer Mechanism, the relevant Transfer will be governed by an unmodified set of EU Model Clauses of which the body is incorporated by reference to this Agreement and the Appendices are attached (**Annex 2).**

(b) **Oracle as Data Processor**. Where Oracle Processes Personal Information on behalf of its customers as a Data Processor, such Personal Information may (depending on the relevant customer agreement) have been Transferred to Oracle or an Oracle Affiliate outside of the EEA under (i) the Oracle BCR-P, (ii) Oracle America, Inc. and its covered Affiliates' Privacy Shield certification, and/or (iii) EU Model Clauses between Oracle (and its Affiliates) and the customer. As the Processing by Supplier and its Authorized Subprocessors may involve Personal Information covered by any of these Transfer Mechanisms, the following applies:

1. **Oracle BCR-P**. Supplier agrees, and shall ensure that its Authorized Subprocessors agree, that where Supplier or any of its Authorized Subprocessors fails to fulfill their data protection related obligations under the Agreement and an Individual has a claim against Oracle or its customer with respect to such violation, but is unable to enforce the claim against Oracle or its customer, because Oracle and/or its customer have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed their entire legal obligations by contract or by operation of law, that the Individual can enforce the data protection related obligations of the Agreement against Supplier and/or Authorized Subprocessor as third-party beneficiaries and that the Individual may, at his or her choice, submit a claim against Supplier and/or the Authorized Subprocessor to the Competent Supervisory Authority or courts in the country of origin of the data Transfer. The parties agree that in such case the relevant Individual shall be entitled to receive compensation for the damage suffered as a result of any breach of the obligations of Supplier and/or its Authorized Subprocessors under the Agreement.

2. **Oracle Privacy Shield**. Supplier shall, and shall ensure that any Authorized Subprocessor shall, Process the relevant Person Information in accordance with the Privacy Shield Obligations.

3. **EU Model Clauses**. Supplier enters into an unmodified set of EU Model Clauses of which the body is incorporated by reference to this Agreement and the Appendices are attached (Annex 2).

3.2 **Restricted Transfers from Argentina**. This Section applies solely when the Processing of Personal Information by Supplier or its Authorized Subprocessors involves a Transfer from Argentina to Supplier or its Authorized Subprocessors located outside Argentina. Such Transfers will be governed by an unmodified set of Argentine Model Clauses of which the body is incorporated by reference to this Agreement, and its Appendix attached (Annex 3).

3.3 **Restricted transfers from other jurisdictions**. Transfers from other jurisdictions globally that have Transfer restrictions are subject to the terms of this SDPA-P, including any data protection and security policies referenced herein.

3.4 **Authorized Subprocessors**. Supplier will provide Oracle with a copy of the relevant Transfer Mechanism and/or related Data Processor provisions with its Authorized Subprocessors promptly upon request. Oracle will have the right to terminate the Agreement if the approved Transfer Mechanism is invalidated and no alternative approved Transfer Mechanism is put in place or when the related Data Processor provisions with its Authorized Subprocessors are not or not adequately put in place.

4. Additional Country-Specific Terms

If additional Processing (including Transfer) requirements are necessary for any specific jurisdiction in order for the Processing by Supplier or its Authorized Subprocessors to be compliant with Applicable Law, Supplier and Oracle shall negotiate in good faith to amend this Agreement to include such requirements and implement these provisions accordingly.

The effective date of this SDPA-P is Effective Date of SDPA-P.

~~**Insert Legal Name Of Supplier**~~	~~**Insert Legal Name Of Oracle Entity**~~
~~By:~~ _____	~~By:~~ _____
~~Name (Print):~~ _____	~~Name (Print):~~ _____
~~Title:~~ _____	~~Title:~~ _____
~~Signature Date:~~ _____	~~Signature Date:~~ _____

ANNEX 1

Key Definitions

For the purposes of this SDPA-P:

1.1. "**Adequacy Decision**" means a decision issued by the European Commission under Applicable law (i.e., Article 25 of the European Data Protection Directive or Article 45 of the GDPR);

1.2. "**Affiliate**" means, as to any entity, any other entity that, directly or indirectly, controls, is controlled by or is under common control with such entity;

1.3. "**Applicable Law**" means any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (including any and all legislative and/or regulatory amendments or successors), to which Supplier or Oracle are subject and which is applicable to Supplier's or Oracle's information protection and privacy obligations;

1.4. "**Argentine Model Clauses**" means the Model Agreement of International Transfer of Personal Data for the case of Provision of Services (*Contrato modelo de transferencia internacional de datos personales con motivo de prestación de servicios*) (reference: EX-2016-00311578- -APN-DNPDP#MJ- Anexo II) approved by the *Dirección Nacional de Protección de Datos Personales* on 2 November 2016;

1.5. "**Binding Corporate Rules**", "**BCR"**, "**Data Controller**", "**Process**", "**Processing**" and "**Data Processor**" have the meaning set out under Applicable Law (e.g., EU Data Protection Directive or GDPR);

1.6. "**BCR-P**" means Binding Corporate Rules for Data Processors;

1.7. "**EEA**" means the European Economic Area and for the purpose of this Agreement, also Switzerland;

1.8. "**EU Model Clauses**" means the standard contractual clauses annexed to the EU Commission Decision 2010/87/EU of 5 February 2010 for the transfer of personal data to processors established in third countries or any successor clauses approved by the EU Commission;

1.9. "**European Data Protection Directive"** means Directive (EC) 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

1.10. "**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);

1.11. "**Individual**" means any identified or identifiable individual about whom Personal Information may be Processed under the Agreement;

1.12. "**Oracle**" and "**Supplier**" mean to refer to the entities that have executed this SDPA-P and the Agreement;

1.13. "**Personal Information**" means any information recorded in any form relating to an Individual or as otherwise defined under Applicable Law;

1.14. "**Privacy Shield**" means the EU-U.S. and/or Swiss-U.S. Privacy Shield Frameworks developed by the U.S. Department of Commerce, the European Commission and Switzerland's Federal Council, including the Privacy Shield Principles and Supplemental Principles (collectively, the "Principles") available at https://www.privacyshield.gov/Privacy-Shield-Principles-Full-Text and http://trade.gov/td/services/odsi/swiss-us-privacyshield-framework.pdf respectively;

1.15. "**Privacy Shield Obligations**" means the Privacy Shield principles and supplemental principles located at https://www.privacyshield.gov, as may be amended from time to time, with the exception for the purpose of this Agreement of providing notice and choice and responding to requests for access and enforcement other than as set out in this Agreement;

1.16. "**Security Incident**" means misappropriation or unauthorized Processing of Personal Information that compromises the confidentiality, security, integrity or availability of the Personal Information;

1.17. "**Special Personal Information**" means any of the following types of Personal Information: (i) social security number, taxpayer identification number, passport number, driver's license number or other government-issued identification number; or (ii) credit or debit card details or financial account numbers, with or without any code or password that would permit access to the account; credit history; or (iii) information on race, religion, ethnicity, sex life or sexual orientation, medical or health information, genetic or biometric information, biometric templates, political opinions, religious or philosophical beliefs, political party or trade union membership, background check information, judicial data such as criminal records or information on other judicial or administrative proceedings; (iv) data of children below the age of 16 years; or (v) any other category of Personal Information identified as special or sensitive under Applicable Law;

1.18. "**Transfer**" means the access by, transfer or delivery to, or disclosure of Personal Information to a person, entity or system located in a country or jurisdiction other than the country or jurisdiction where the Personal Information originated from; and

1.19. "**Transfer Mechanism(s)**" means Binding Corporate Rules, Privacy Shield, EU Model Clauses, Argentine Model Clauses and any other transfer mechanism required to undertake a Transfer.

ANNEX 2

Appendix 1 to EU Model Clauses (description of transfer)

Data Exporter and Data Importer

The Data Exporter transfers, and Data Importer receives, Personal Information in relation to the supply of Services as set out in the relevant Services Contract.

Data subjects

Employees, including temporary and prospective employees, relatives, guardians and associates of the data subject, existing and prospective customers, suppliers, visitors or registrants at offices, web sites and/or events, employees of corporate business associates (e.g., resellers of company products and services), advisors, consultants and other professional experts, and/or other categories as set out in the relevant Services Contract.

Categories of data

Personal contact details including name, home address, home telephone or mobile number, fax number, email address, and passwords, family, lifestyle and social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or children, employment details including employer entity name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, and business contact details, results from background checks, administrative, audit, accounting and financial information, including tax information and bank details, information gathered in connection with investigations such as video footage and ID badge records, network, computer, email and phone or other communications or messaging systems, logs, data and files, including network traffic data and domain names of websites visited, emails and files stored in company workspaces, imaging and forensic analysis of computing resources and any data stored on those resources, personal data about individuals named in legal matters or correspondence, or provided in connection with the provision of legal, banking, audit and/or financial services, including for conflict checking and billing purposes, financial details, goods and services provided, browser and device information, data collected through automated electronic interactions, application usage data, demographic information, geographic or geo-location information, and/or other data as set out in the relevant Services Contract.

Special Categories of data (if appropriate)

Data regarding racial or ethnic origin, political opinions, religious or other beliefs of a similar nature, trade union membership, sexual life, physical health or mental condition, offenses or alleged offenses, and/or other sensitive information as set out in the relevant Services Contract.

Processing operations

Processing operations are limited to the extent necessary to provide the services as specified under the Services Contract.

~~Data Importer:~~ **~~Insert Name Of Supplier~~**	~~Data Exporter:~~ **~~Insert Name Of Oracle Entity~~**
~~By:~~ _____	~~By:~~ _____
~~Name (Print):~~ _____	~~Name (Print):~~ _____
~~Title:~~ _____	~~Title:~~ _____
~~Signature Date:~~ _____	~~Signature Date:~~ _____

Appendix 2 to EU Model Clauses (security)

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Data Importer shall comply with the techincal and organisational security measures as set forth in the OSSS.

ANNEX 3

Annex A to Argentine Model Clauses

[GLOBAL STANDARD - DO NOT CHANGE EITHER COLUMN TO LOCAL LANGUAGE – KEEP AS IS]

Titulares de los datos	**Data owners**
Los datos personales transferidos se refieren a las siguientes categorías de titulares de los datos: Consulte *La descripción de la transferencia* adjunta.	The personal data transferred concern the following categories of data owners: *Please refer to the attached "Description of Transfer" document(s)*
Características de los datos	**Characteristics of the data**
Los datos personales transferidos se refieren a las siguientes categorías de datos: Consulte *La descripción de la transferencia* adjunta.	The personal data transferred concern the following categories of data: *Please refer to the attached "Description of Transfer" document(s)*
Tratamientos previstos y finalidad	**Purpose of the data processing to be conducted:**
Los datos personales transferidos serán sometidos a los siguientes tratamientos y finalidades: Consulte *La descripción de la transferencia* adjunta.	The transferred personal data will be subject to the following processing and purposes: *Please refer to the attached "Description of Transfer" document(s)*

Data Importer

~~By:~~ _____

~~Name (Print):~~ _____

~~Title:~~ _____

Company: [**Insert Legal Name of Supplier**]

Address and Country of Establishment: [**Insert Address and Country of Supplier**]