MASTER DATA PROCESSING AGREEMENT

(pursuant to Article 28 of Regulation EU 2016/679)

BETWEEN

This agreement for the protection of personal data is entered into between the Provider, as indicated below, and the client, who accepts the agreement. "**Provider**" indicates the following entity:

Reviso Cloud Accounting Limited, 1st Floor, Healthaid House Marlborough Hill Harrow Middlesex HA1 1UD, United Kingdom

AND

the entity referred to in the Agreement as the client (hereinafter the "**Client**")

hereinafter collectively referred to as the "**Parties**" or individually as the "**Party**".

WHEREAS:

a) The Client has entered into an agreement (or agreements) with the Provider (hereinafter referred to as the "**Agreement**").
b) In this "*master data protection agreement*" (hereinafter referred to as the "**Master Agreement**" or "**MDPA**") the Parties wish to establish how and upon which conditions the Provider will process personal data in connection with the Agreement and the provision of the Services, as well as its obligations relating to such processing, including the duty of the Provider as a Data Processor under Article 28 of the General Regulation on Data Protection No. 679 of 27 April 2016 (hereinafter "**GDPR**").
c) The specific characteristics of the processing activity in respect to each of the Services are detailed in the "special terms and conditions for the processing of Personal Data" that are available on the website: https://www.reviso.com/gdpr/(hereinafter "**DPA - Special Terms**") and are incorporated herein by this reference.

NOW THEREFORE, the Parties hereto agree as follows:

1. DEFINITIONS AND INTERPRETATION

1.1. The above recitals are hereby incorporated into this MDPA by this reference. As used in this MDPA the following words and expressions shall have the meanings set forth below:

"Adequacy Decision" means a decision of the European Commission, based on Article 45(3) of the GDPR, assessing that the laws of a certain country ensure an adequate level of protection, as required by the Applicable Data Protection Law.

"Applicable Data Protection Law" means applicable data protection legislation as amended, which includes i.a. the GDPR and any other implementing law and/or regulation (if any) which is effective under the GDPR or otherwise with respect to the protection of Personal Data, including any decision issued by a supervisory authority having jurisdiction in the subject matter that is and remains binding and effective (including the requirements established in any General Authorizations Issued for the Processing of Sensitive and Judicial Data, to the extent that they are applicable and remain effective and binding after 25 May 2018).

"Data Sub-Processor" means any sub-contractor engaged by the Provider to perform, in full or in part, its contractual obligations and which, during such performance, may be required to collect, access, receive, store, or otherwise process Personal Data.
"E-mail Address" means the e-mail address(es) provided by the Client upon subscription of the Services or communicated via other official means to the Provider, at which the Client wishes to receive communications from the Provider.
"Final User" means the person (if any) benefiting of the Services in the last resort, acting as Data Controller.
"Instructions" means the written instructions given by the Data Controller in this MDPA (including the relevant DPA – Special Terms) and, if any, in the Agreement.
"MDPA Effective Date" means the date when the Client signs or accepts the MDPA or the effective date of the MDPA to which this Agreement is related, whichever is earlier.
"Personal Data Breach" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data occurred on the systems operated by the Provider or however under its control.
"Personal Data" has the meaning construed according to the Applicable Data Protection Law and include, without limitation, all personal data provided, stored, transmitted, received or otherwise processed, or created, by the Client, or by the Final User in relation to the provision of the Services, to the extent that they are processed by the Provider under the Agreement. A list of the categories of Personal Data is included in DPA – Special Terms.
"Personnel of the Provider" means the officers, employees, consultants, and other personnel of the Provider but not the personnel of a Data Sub-Processor.
"Request" means a request lodged by a Data Subject for access, erasure or rectification in relation to his/her Personal Data or for the exercise of another of his/her rights laid down in the GDPR.
"Service(s)" means the service or services contemplated in the Agreements executed from time to time between the Client and the Provider.
"Working Days" means every calendar day other than a Saturday, Sunday and a Bank or Public Holiday in the UK.

1.2. The words "including" or "included" shall be construed as if they were accompanied by the expression "without limitation" so that any list that follows any of these words will consequently be composed of mere examples and will not be exhaustive.

1.3. For the purposes of this MDPA, the terms "Data Subject", "Processing", "Data Controller", "Data Processor", "Transfer" and "Appropriate Technical and Organizational Measures" shall be construed in compliance with the Applicable Data Protection Law.

2. ROLES OF THE PARTIES

2.1. The Parties acknowledge and agree that, in relation to the processing of Personal Data, the Provider acts as the Data Processor and, as a general rule, the Client acts as the Data Controller.

2.2. If the Client is carrying out the processing on behalf of another Data Controller, the same Client may act as a Data Processor. In such event, the Client hereby represents and warrants that all instructions given and activities carried out in relation to the processing of Personal Data, including the appointment of the Provider as a Data Sub-Processor, arising from the execution by the Provider of this MDPA, has been authorized by the relevant Data Controller. The Client shall give evidence to the Provider, upon written request by this latter, of the above.

2.3. In the processing of Personal Data, either Party undertakes to comply with their obligations under the Applicable Data Protection Law.

3. PROCESSING OF PERSONAL DATA

3.1. By entering into this Agreement (and into any incorporated DPA – Special Terms), the Client entrusts the Provider with the processing of Personal Data for the purposes of providing the Services, as better detailed in the Agreement and in the DPA – Special Terms. The DPA – Special Terms are available at a link on the following website: www.reviso.com/gdpr .

3.2. The Provider may only process Personal Data on behalf of the Client based on its Instructions, unless required to do so by EU law or EU member state law to which the Provider is subject; in such a case, the Provider shall inform the Client of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Should the Client make a request for amendments to any initially given Instructions, the Provider will examine the relevant feasibility and will then arrange with the Client how to handle such amendments and the associated costs.

3.3. The Provider shall immediately inform the Client if, in its opinion, an Instruction infringes Applicable Data Protection Law, and the Provider shall be released from any obligations to perform such unlawful Instructions. In such case, the Client may consider whether amending the Instructions given or addressing the Supervisory Authority to have its requests be declared lawful.

4. RESTRICTIONS TO THE USE OF PERSONAL DATA

4.1. While processing Personal Data for the purposes of providing the Services, the Provider undertakes that such processing shall be carried out:

4.1.1. Only to the extent and with the manners that are necessary to provide the Services, or to properly perform its obligations under the Agreement and this MDPA, or laid down by the law or by a competent supervisory or controlling authority. In this last case, the Provider must inform the Client (unless prevented to do so by the applicable law based on the public interest) by a notice to the E-mail Address.

4.1.2. In compliance with the Instructions of the Client.

4.2 The Personnel of the Provider having access to, or however carrying out the processing of, Personal Data has been entrusted with such processing based on appropriate authorizations and has also received training as necessary with respect to such processing. In addition, this Personnel is bound to comply with confidentiality obligations and with the Provider's Code of Ethics and must abide by the policies on confidentiality and personal data protection that have been adopted by the Provider.

5. PROCESSING ACTIVITIES ENTRUSTED TO THIRD PARTIES

5.1. As far as concerns the processing activities entrusted to Data Sub-Processors, the Parties agree as follows:

5.1.1. The Client expressly agrees that the Provider may entrust certain processing operations in relation to Personal Data to other companies belonging to the TeamSystem group and/or to those third parties that are specified in the DPA – Special Terms, provided the requirement in para. 5.1.4.3 is complied with.

5.1.2. The Client further agrees that the Provider may entrust certain processing operations in relation to Personal Data also to other third parties, according to the requirements specified in the par. 5.1.4.

5.1.3. It is noted that the execution of Standard Contractual Clauses (as required by the following Article 7 for the case of transfer of Personal Data abroad) between the Client and a Data Sub-Processor shall be deemed as a consent to engaging that party for the processing activities.

5.1.4. If the Provider changes or engages Data Sub-Processors for performing specific processing activities in relation to Personal Data under the MPDA, the Provider:

5.1.4.1. Undertakes to engage exclusively Data Sub-Processors granting implementation of appropriate technical and organizational measures and ensures that the access to Personal Data, and the relevant processing, shall be limited only to that extent that it is necessary for the purposes of providing the sub-delegated services.

5.1.4.2. Shall inform the Client of such changes or engagement, by giving not less than 15 (fifteen) days' notice prior to the start of the processing activities by the Data Sub-Processor (including details concerning the identity of the concerned third party, its location with –if applicable- specification of the location of the servers for the storage of data, and the entrusted activities) by means of the E-mail Address or such other means as deemed appropriate by the Provider. The Client shall be entitled to terminate from the Agreement within 15 (fifteen) days from receipt of the notice, without prejudice to the obligations of the Client to pay any amounts due at the date of termination of the Agreement.

5.1.4.3. enters into a written agreement with each Data Sub-Processor which imposes the same obligations on the Data Sub-Processor's as are imposed on the Provider under this MDPA.

5.1.5. Additional information concerning the list of Data Sub-Processors, the processing activities entrusted to such parties and the place where they are located are available in the DPA – Special Terms relating to the Services activated by the Client.

5.1.6. The Provider shall remain fully liable to the Client for the performance of the Data Sub-Processor's delegated data protection obligations related to this MDPA.

6. SECURITY

6.1. *SUPPLIER'S SECURITY MEASURES* – When processing Personal Data for the purposes of performing the Services, the Provider undertakes to implement appropriate technical and organizational measures to prevent unlawful or unauthorized processing, accidental or unlawful destruction, damages, accidental loss, alteration and unauthorized disclosure of, or access to, Personal Data, as described in Exhibit 1 to this MDPA ("**Security Measures**").

6.1.1. Exhibit 1 to the MDPA sets forth appropriate measures for the protection of filing systems that are proportionate to the level of risk in relation to Personal Data, in order to ensure the confidentiality, integrity, availability and resilience of the systems and of the Services of the Provider, appropriate measures aimed at enabling restoration of access to Personal Data in a timely manner in the event of a Personal Data Breach, and measures aimed at regularly testing the effectiveness of such measures in the course of time. The Client acknowledges and accepts that, account taken of the state of the art, the costs of

implementation and the nature, scope, context and purposes of Personal Data processing, the security procedures and principles that have been adopted by the Provider ensure a level of protection that is appropriate to the risk in relation to Personal Data.

6.1.2. The Provider may update and amend the Security Measures specified above from time to time, provided that such updating and amendments do not imply a reduction of the overall level of security of the Services. The Client shall be informed of any such update and amendment by notice transmitted to the E-mail Address.

6.1.3. If the Client requests additional measures for the security, other than Security Measures, the Provider reserves the right to assess the relevant feasibility and may charge additional costs of implementation to the Client.

6.1.4. The Client acknowledges and accepts that the Provider, account taken of the nature of Personal Data and information that is available to the Provider itself based on the specific provisions established in the relevant DPA – Special Terms, shall assist the Client in ensuring compliance with the obligations set forth in Articles from 32 to 36 of the GDPR, including e.g. by:

6.1.4.1. By implementing and keeping Security Measures updated according to the provisions set forth in previous paragraphs 6.1.1, 6.1.2, 6.1.3.

6.1.4.2. By complying with the obligations specified in paragraph 6.3.

6.1.5. The Parties hereby agree that, with reference to the Agreements concerning products to be installed on the premises of the Client or of any suppliers of the Client (hereinafter "***On-premises* Products**"), the above Security Measures shall only apply in connection with Services that require the processing of Personal Data by the Provider or by any Data Sub-Processors engaged by this latter (*e.g.* remote support and assistance, migration services).

6.1.6. In case that the product admits integration with applications of third parties, the Provider shall not be liable for the implementation of the Security Measures in relation to the components of such third parties or for any product's operating manner consequent to such integration.

6.2. *CLIENT'S SECURITY MEASURES* – Without prejudice to the obligations of the Provider under paragraph 6.1 above, the Client acknowledges and accepts that, when using the Services, it remains an exclusive duty of the Client to have its personnel, and those authorized by the same Client to access the Services, implement appropriate security measures in connection with the use of the Services.

6.2.1. To this purpose, the Client undertakes to use the Services and the features for the processing of Personal Data by always ensuring a level of security appropriate to actual risk.

6.2.2. The Client further undertakes to implement all appropriate measures for ensuring the protection of authentication credentials, systems, and devices used by the Client, or by the users of the Final User, to gain access to the Services. The Client also undertakes to save and make backup copies of Personal Data in order to ensure their restoration in compliance with the provisions of the laws.

6.2.3. The Provider shall have no obligation and shall bear no liability in relation to the protection of Personal Data that the Client, or –if applicable- the Final User, store or transfer outside the systems used by the Provider or by the Data Sub-Processors engaged

by the Provider (for instance in paper archives, or in data centres belonging to the Client or the Final User, as it may occur in case of Agreements concerning On-premises Products).

6.3. *DATA BREACHES* – Save for the Agreements concerning On-premises Products, to which this paragraph 6.3 shall not apply, the Provider, after having become aware of a Personal Data Breach, shall:

6.3.1. Inform the Client without undue delay via the E-mail Address.

6.3.2. Adopt reasonable measures to mitigate any damages possibly arising from it and protect Personal Data.

6.3.3. Provide the Client with a description of the Personal Data Breach, to the extent possible, including the measures taken to prevent or mitigate its possible adverse effects and the activities recommended by the Provider to the Client in order to address the Personal Data Breach.

6.3.4. Keep all information concerning Personal Data Breaches, the relevant documents, communications and notices, confidential as provided for in the Agreement and abstain from disclosing any data and information to third parties without the prior written authorization of the Data Controller, save and to the extent that such disclosure may be strictly necessary to perform any Client's obligations arising from the Applicable Data Protection Law;

6.3.5. Provide such other information and assistance as are required in relation to Personal Data Breaches by Applicable Data Protection Law.

6.3.6. In the cases contemplated under previous paragraph 6.3, the Client shall be exclusively liable for the performance, when required by the Applicable Data Protection Law, of any obligations to inform third parties (or the Final User if the Client is the Data Processor) in case of a Personal Data Breach and of any obligations to inform the Supervisory Authority and the Data Subjects (if the Client is the Data Controller).

6.4. The Parties acknowledge and accept that a communication about a Personal Data Breach or the implementation of measures aimed at addressing such a Personal Data Breach do not imply acknowledgment by the Provider of a default or a liability in relation to the Personal Data Breach.

6.5. The Client shall timely inform the Provider of any abuse or misuse of the accounts or authentication credentials or of any Personal Data Breaches of which it may have become aware in relation to the Services.

7. RESTRICTIONS TO THE TRANSFER OF PERSONAL DATA TO COUNTRIES OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

7.1. The Provider shall not transfer Personal Data to countries that are outside the EEA unless the Client gives its consent and Instruction to such a transfer.

7.2. If the Client gives its consent and Instruction to process Personal Data outside EEA pursuant to para. 7.1, and in the absence of a decision of adequacy by the European Commission on that country pursuant to Article 45 of the GDPR, the Provider:

7.2.1. Shall make the Data Sub-Processor execute the Standard Contractual Clauses contemplated in the Commission Decision 2010/87/EU of 5 February 2010, for the transfer of personal data to processors established in third countries ("**Standard**

Contractual Clauses"), or equivalent text, as it may be lately amended. A copy of such Standard Contractual Clauses executed by the Provider on behalf of the Client pursuant to para. 7.3 shall be provided to this latter. And/or

7.2.2. May submit alternative ways to the Client for the transfer of Personal Data that are compliant with the requirements of the Applicable Data Protection Law (*e.g.* intragroup transfer if the Data Sub-Processor belongs to a group of companies whose BCRs have been approved in relation to the Processors).

7.3. In the events under previous paragraph 7.2.1, by execution of this MDPA the Client expressly grants the Provider with the authority to execute Standard Contractual Clauses or others approved by Client pursuant to clause 7.1 or similar to cater for future third country transfers with the Data Sub-Processors mentioned in the relevant DPA – Special Terms. If the Final User acts as a Data Controller, the Client undertakes to inform such Final User of the transfer and hereby represents and warrants that the authorization given by such Final User to engage Data Sub-Processors outside the EEA represents an authority equivalent to that above.

8. AUDITS AND CONTROLS

8.1. The Provider shall make available to the Client all information necessary to demonstrate compliance with the obligations laid down in this MDPA. In this context, the Provider shall regularly audit the security of the Personal Data processing systems and environments used by it to perform the Services as well as the premises where the processing is carried out. The Provider may decide to select and entrust certain independent consultants with performing such audits, which shall be made according to international standards and/or best practices and whose outcome shall be described in special reports ("**Reports**"). The Reports, to be deemed as confidential information of the Provider, may be made available to the Client for allowing verification by this latter of the Provider's compliance with the security obligations set forth in this MDPA.

8.2. In the cases contemplated in paragraph 8.1, the Client hereby accepts to exercise its right to verification simply by accessing the Reports made available to it by the Provider.

8.3. Despite para. 8.2, the Provider acknowledges that the Client is entitled, with the manners and to the extent specified below, to carry out independent audits in order to verify the compliance of the Provider with the obligations of this MDPA and the relevant DPA – Special Terms, and with the provisions of the Applicable Data Protection Law. For performing such auditing activities, the Client may decide to avail of specialized employees or, at its choice, of external consultants provided that these latter shall be previously bound by appropriate confidentiality obligations.

8.4. In the cases contemplated in paragraph 8.2 above, the Client must address a prior request to the Data Protection Officer (DPO) of the Provider. Upon such a request for an audit or an inspection, the Provider and the Client shall agree, prior to the start of the activities, the details of the verification activities (starting date and duration), the types of controls and the scope of verification, the confidentiality obligations by which the Client and those performing the activities must be bound, and the costs, to be established based on the width and length of the verification activities, which the Provider is entitled to charge for such activities.

8.5. The Provider is entitled to object, by means of written notice, in the event that the external auditors appointed by the Client, in the exclusive opinion of the Provider, do not meet adequate qualification or independence requirements, are competitors of the Provider, or are

clearly unfit. In any such event, the Client must appoint new auditors or directly carry out the audits on its own.

8.6. The Client undertakes to bear the costs, if any, as they may be determined by the Provider and communicated to the Client according to paragraph 8.4 above, in the manners and within the terms established therein. All costs relating to any verification activities entrusted by the Client to third parties shall remain fully and exclusively at the charge of the Client.

8.7. All the above is without prejudice to the rights of the Data Controller and of the supervisory authorities as established in the Standard Contractual Clauses executed under previous Article 7 (if any), which shall not be affected by any provisions set forth in this MDPA or in the relevant DPA – Special Terms.

8.8. This Article 8 shall not apply to the Agreements concerning On-premises Products.

8.9. Verification activities involving any Data Sub-Processors shall be carried out in compliance with the rules on access and with the security policies established by such Data Sub-Processors.

9. ASSISTANCE IN ENSURING COMPLIANCE

9.1. The Provider shall assist the Client and provide cooperation as specified below to enable the Client to comply with its obligations under the Applicable Data Protection Law, including e.g. in relation to responding to Requests pursuant to GDPR Chapter III.

9.2. In case that the Provider receives a Request or a claim concerning Personal Data from a Data Subject, it shall invite this latter to address the Request or claim to the Client or the Final User (if this latter is the Data Controller). In any such event, the Provider shall timely inform the Client of the reception of the Request via the E-mail Address and provide the same Client with all available information, together with a copy of the Request or claim. This cooperation will be carried out by way of an exception to the general rule that the relationships with the Data Subjects fall outside the scope of the Services and that the responsibility to handle claims (if any) and to serve as a contact for Data Subjects in the exercise of their rights lies exclusively and directly with the Client or with the Final User (if this latter is the Data Controller). The Client, or Final User (if this latter is the Data Controller) shall be exclusively responsible for any response to such Requests or claims (if any).

9.3. The Provider shall promptly inform the Client, unless it is prohibited by the law to do so, by means of a notice via the E-mail Address, of any inspections or requests to provide information that it receives from any supervisory or police authorities in relation to the processing of Personal Data.

9.4. If in order to comply with any such Request the Client needs to receive some information from the Provider about the processing of Personal Data, the Provider shall provide assistance to the extent that is reasonably possible, provided that the requests have been filed upon adequate notice.

9.5. The Provider, account taken of the nature of the Personal Data and of the information available to him, shall give reasonable assistance to the Client in making available useful information to enable the Client to carry out the impact assessments on the protection of Personal Data when so required by the law. In such cases the Provider shall make general information available, based on the Service, such as information included in the Agreement, in this MDPA and in the DPA – Special Terms relating to the concerned Services. In case of requests for customized assistance, the Client may be required to pay a charge. It is the exclusive responsibility of the Client, or the Final User (if this latter is the Data Controller), to carry out the impact assessment

based on the characteristics of Personal Data processing performed by the same with respect to the Services.

9.6. The Provider undertakes to provide the Services based on the principles of minimization of the processing (privacy by design & by default), without prejudice to the fact that it is the responsibility of the Client, or of the Final User (if this latter is the Data Controller), to ensure that the processing is actually carried out in compliance with such principles and to verify that the technical and organizational measures of a Service will meet the compliance requirements of the Client, or if the Final User (if this latter is the Data Controller), including requirements established by the Applicable Data Protection Law.

9.7. The Client acknowledges and accepts that, in case of a Request by a Data Subject for the portability of Personal Data, and with exclusive reference to the Services generating Personal Data that are relevant in this respect, the Provider shall assist the Client by making available the information needed for retrieval of the required data in a format that is compliant with the Applicable Data Protection Law.

9.8. Paragraph 9.5 and 9.7 shall not apply with respect to any Agreements concerning On-premises Products.

10. OBLIGATIONS OF THE CLIENT AND RESTRICTIONS

10.1. The Client undertakes to give Instructions in compliance with the regulations and to use the Services in compliance with the Applicable Data Protection Law and for the exclusive purpose of processing Personal Data that have been collected in compliance with the Applicable Data Protection Law.

10.2. The processing of Personal Data (if any) under Article 9 and Article 10 of the GDPR shall be allowed only if expressly established in the DPA – Special Terms. But for such cases, the processing of Personal Data contemplated in the articles mentioned above shall be made exclusively upon prior written agreement between the Parties made in compliance with the provisions of paragraph 3.2.

10.3. The Client undertakes to fulfil all the obligations placed upon the Data Controller pursuant to the Applicable Data Protection Law (and, in the event that such obligations are placed upon the Final User, it ensures that an equivalent commitment is taken on by such Final User), including the obligations to provide certain information to the Data Subjects (and it ensures that equivalent obligations are placed upon the Final User if this latter is the Data Controller). The Client further undertakes to ensure that the processing of Personal Data by availing of the Services shall always be made upon a suitable legal basis.

10.4. If the information notice must be given and the consent must be collected by means of the product contemplated in the Agreement, the Client declares to have considered the product and that such product meets the needs of the Client. The Client shall also bear the responsibility to assess whether the forms made available by the Provider (if any) to help the Client in meeting its obligations to inform and to collect the consent (*e.g.* model privacy policy for Apps or information notices accompanying applications), when made available, complies with the Applicable Data Protection Law and amend such forms if deemed appropriate.

10.5. The Client shall further bear full and exclusive responsibility for handling the Personal Data in compliance with the Requests (if any) submitted by the Data Subjects and, therefore, to carry out –for instance- any amendments, integration, rectification and erasure of Personal Data.

10.6. The Client has the duty to keep the account associated with the E-mail Address always active and updated.

10.7. The Client acknowledges that, according to Article 30 of the GDPR, the Provider has the duty to maintain a record of the processing activities carried out on behalf of the Data Controllers (or Processors) and that for this purpose it collects the identification and contact data of each Data Controller (and/or Processor) on behalf of which it acts and that such information must be made available to the competent authority, upon request. Therefore, whether so requested, the Client undertakes to give the Provider the identification and contact data mentioned above, with the manner specified by the Provider from time to time, and to maintain updated such information through the same means.

10.8. Therefore, the Client states and declares that the processing of Personal Data, as described in the Agreements, in this MDPA and in the relevant DPA – Special Terms, is lawful.

11. DURATION

11.1. This MDPA shall enter into force on the Effective Date of the MDPA and will automatically terminate at the date of return/erasure of all Personal Data by the Provider, as provided for in this MDPA and, if so provided for, in the relevant DPA – Special Terms or the Agreement.

12. PROVISIONS ON THE RETURN OR ERASURE OF PERSONAL DATA

12.1. Upon termination, for whatever reasons, of the Service, the Provider will cease the processing of Personal Data and

12.1.1. Erase Personal Data (including the relevant copies, if any) from the systems of the Provider or that are under the Provider's control, within the term established in the Agreement, unless retention of such data is required or permitted in order to comply with any provisions of European laws.

12.1.2. Destroy any Personal Data that may have been stored on paper by the same Provider, unless retention of such data is required in order to comply with any provisions of European laws.

12.1.3. Keep at the Client's disposal the Personal Data for the extraction for the period of the Contract. If the Contract does not provide for a specific time limit, the Supplier shall keep the Personal Data available to the Client for the period of 60 (sixty) days after the termination of the Contract.

12.2 Unless otherwise provided for in this MDPA, the Client acknowledges that it is allowed, after termination of the Service, to retrieve Personal Data in the manners specified in the Agreement and agrees on its duty to retrieve Personal Data, in full or in part, to the exclusive extent that it deems retention appropriate, and that such retrieval must be completed within the term specified in paragraph 12.1.3.

12.3 The Parties agree that the provisions in paragraphs 12.1 and 0 shall not apply to Agreements concerning On-premises Products. In these cases, the Client has the duty to retrieve those Personal Data that it deems appropriate for storage, not later than 30 (thirty) days after the end of the Agreement. The Client acknowledges and accepts that after expiration of this term Personal Data may become unavailable. Furthermore, in the events considered in this paragraph 0, it is the duty of the Client to take care of the erasure of Personal Data as required by the law.

12.4 The above is without prejudice to what, which may be further or otherwise established with respect to the erasure of Personal Data in the relevant DPA – Special Terms.

13. LIABILITY

13.1. Either Party is liable for the fulfilment of the obligations placed upon that Party under this MDPA and the relevant DPA – Special Terms as well as under the Applicable Data Protection Law.

13.2. Without prejudice to mandatory law provisions, the Provider shall compensate the Client in case of breach of this MDPA and/or of the relevant DPA – Special Terms within the maximum extent agreed upon in the Agreement.

14. MISCELLANEOUS

14.1. This MDPA supersedes and replaces any other agreement, contract, or understanding between the Parties with respect to its subject matter as well as any instructions, in any form, given by the Client to the Provider prior to the date of this MDPA with reference to the processing of Personal Data in the framework of performing the Agreement.

14.2. The Provider may amend this MDPA by means of written notice to be sent to the Client (via e-mail or with the help of computer programs or otherwise). In this event, the Client will be entitled to withdraw from the Agreement by written notice to the Provider to be sent by registered letter with return receipt within 15 days from receipt of the Provider's notice. Failing exercise by the Client of this right of withdrawal within the terms and in the manners as described above, the amendments to this MDPA shall be deemed as acknowledged and accepted by the Client and will become finally effective and binding on the Parties.

14.3. In the event of any inconsistency between the provisions of this MDPA and those set forth in the Agreement for the provision of the Services or in any documents of the Client that have not been expressly accepted by the Provider by departing from this MDPA and/or from the respective DPA – Special Terms, the provisions of this MDPA and of the relevant DPA – Special Terms shall prevail.

15. GOVERNING LAW AND VENUE

15.1 This DPA shall be construed in accordance with the laws of Italy and each party hereby irrevocably submits to the non-exclusive jurisdiction of the courts of Milan (Italy), without application of any conflicts of law provisions.

Exhibit 1

Technical and organisational measures

In addition to the security measures set forth in the Agreement and in the MDPA, the following organizational security measures shall be applied by the Data Controller based on the type of Service through which the product is delivered or licensed:

A – Cloud SaaS
B – Iaas Services
C – BPO (Business Process Outsourcing)
D – BPI (Business Process Insourcing)
E – On premises

A – CLOUD SaaS

Organizational Security Measures	*User Policies and Regulations* – The Provider has adopted detailed policies and regulations, which all users having access to information systems must comply with, aimed at granting that users' behaviour is appropriate to ensure compliance with the principles of confidentiality, availability and integrity of data while using information resources. *Logical access authorization* – The Provider defines access profiles based on the least privilege necessary to carry out the assigned duties. The authorization profiles are selected and configured prior to the beginning of the processing and in such a manner that access will be restricted only to those data that are strictly necessary for the processing activities. The profiles undergo regular audits aimed at assessing whether the requirements to maintain the assigned profiles are still met. *Assistance Interventions* – Assistance interventions will be managed with the aim of ensuring that only contractual activities are performed and that any unnecessary processing in relation to Personal Data of the Client or of the Final User is prevented. *Data Protection Impact Assessment (DPIA)* – In compliance with Articles 35 and 36 of the GDPR and based on the document "WP248 – Guidelines on Data Protection Impact Assessment", adopted by the Article 29 Working Party, the Provider has prepared its own methodology for the analysis and assessments of those processing activities that, taking into account the nature, scope, context and purposes of the processing, are likely to result in a high risk for the rights and freedoms of natural persons, in order to be able to carry out an

	assessment of the impact on the protection of personal data prior to the processing. *Incident Management* – The Provider has adopted a specific Incident Management procedure aimed at ensuring restoration of the ordinary service operations at the soonest while ensuring to maintain best service levels. *Data Breach* – The Provider has implemented a special procedure, aimed at the management of events and incidents that are likely to have an impact on personal data, which defines the roles and responsibilities, the process for detection of the (suspected or actual) incident/breach, the implementation of remedial actions, the response to, and containment of, such incident/breach as well as the formalities to inform the Client of personal data breaches. *Training*: The Provider will periodically offer training courses on proper handling of personal data to members of its personnel that are involved in the processing activities.
Technical Security Measures	*Firewall, IDPS* – Personal data shall be protected against the risk of a criminal intrusion by means of Intrusion Detection & Prevention Systems (IDPS), to be kept updated based on the best available technologies. *Security of communication lines* – Within the extent of its responsibilities, the Provider shall implement secure communication protocols that are in line with the available technology. *Protection from malware* – The systems shall be protected against the risk of an intrusion and of the activity of certain programs by activation of appropriate electronic tools to be periodically updated. Antivirus features shall be implemented and kept constantly updated. *Authentication Credentials* – The systems shall be configured in such a manner that access will be granted exclusively to those provided with authentication credentials allowing unique identification of the user. This include: a code associated to a confidential password that shall only be known by the user, or an authentication device that shall only be held and used by the user, which may, in certain cases, be associated with an ID code or a password. *Password* – The use of a password, as far as concerns its basic features, being the obligation to change it at the first access, the minimum length, the absence of elements that may be easily referred to its holder, the rules about its complexity, the expiration, history, assessment of strength in context, display and storage, will comply with the best practices. Users being provided

	with credentials shall also receive specific instructions concerning the measures that must be adopted to ensure that such credentials remain secret. *Logging* – The systems may be configured in such a manner as to track access requests and, where appropriate, other activities that are carried out, in relation to the different types of users (Administrator, Super User, etc.), and shall be protected by appropriate security measures ensuring their integrity. *Backup & Restore* – Appropriate measures shall be implemented aimed at ensuring restoration of access to data in case of damages to such data or to electronic tools, within terms that are certain and consistent with the rights of the data subjects. If so required by any agreement, a continuity operation plan shall be implemented and, where necessary, integrated with the disaster recovery plan. These plans ensure the availability and access to the systems also in the event of serious adverse events that may persist in time. *Vulnerability Assessment & Penetration Test* – The Provider shall regularly carry out vulnerability analyses aimed at assessing the level of exposure to known vulnerabilities, in relation to both the infrastructures and the operations framework, taking into account either already operating systems and systems that are under development. When deemed appropriate, in relation to those potential risks that have been identified, the assessments above are complemented, from time to time, by special Penetration Test technics, simulating unauthorized access in various scenarios of attack, with the aim of controlling the level of security attained by applications/systems/networks by using the identified vulnerabilities to circumvent the physic/logic security mechanisms and gain access to them. The outcome of such assessments is thoroughly examined in order to detect and implement improvements that are necessary to ensure the high level of security that is required. *System Administrators* – All users operating as System Administrators shall be indicated in a list to be regularly updated and the duties assigned to them shall be duly defined in special documents of appointment. The activity performed by System Administrators shall be monitored by means of a log management system allowing to accurately trace all performed activities and to store such data in an immutable manner in order to allow the monitoring also after performance. The behaviour of System Administrators shall be audited to verify compliance with the organizational, technical and security measures in relation to the processing of personal data as required by current regulations.

	Data Centre – The physical access to the Data Centre is restricted to authorized persons only. For further details on the security measures adopted in relation to the data centre services provided by the Data Sub-Processor specified in the DPA – Special Terms please refer to the descriptions of such security measures prepared by the same Data Sub-Processors and made available in the relevant official sites, at the address specified in the following (or at the address that may be made available in the future by the same Data Sub-Processors): With reference to Data Centre services provided by Amazon Web Services: https://aws.amazon.com/it/compliance/data-center/controls/ With reference to Data Centre services provided by Microsoft: https://www.microsoft.com/en-us/trustcenter

B – Iaas Services

Organizational Security Measures	*Certifications* – The Provider has obtained the following certifications/assessments: • ISO/IEC 27001:2013: "Delivery of services for the design and management of ICT infrastructure, management of applications within the Group and management of Cloud infrastructure (IaaS)". • ISO/IEC 27018:2014 for the protection of personal data in Public Cloud services. *Logical access authorization* – The Provider defines access profiles based on the least privilege necessary to carry out the assigned duties. The authorization profiles are selected and configured prior to the beginning of the processing and in such a manner that access will be restricted only to those data that are strictly necessary for the processing activities. The profiles undergo regular audits aimed at assessing whether the requirements to maintain the assigned profiles are still met. *Users* – Users of the services are divided into administrative users of the virtualization infrastructure and administrative users of the console for the management of TeamSystem cloud infrastructure. The VMs shall be configured in such a manner that access will be granted exclusively to those provided with authentication credentials allowing unique identification of the user. *Security of communication lines* – Within the extent of its responsibilities, the Provider shall implement secure communication protocols that are in line with the available technology in relation to the authentication process. *Change Management* – The Provider has implemented a specific procedure to regulate the Change Management process in view of the introduction (if any) of technological innovations or in case of modifications (if any) of its basic and organizational structure.

	Training: The Provider will periodically offer training courses on proper handling of personal data to members of its personnel that are involved in the processing activities. *Protection from malware* – The VMs shall be protected against the risk of an intrusion and of the activity of certain programs by activation of appropriate electronic tools to be periodically updated. All VMs shall be managed through antivirus features (at both hypervisor and infrastructure level). *Backup & Restore* – If so required by any agreement, appropriate measures shall be implemented aimed at ensuring restoration of access to data in case of damages to such data or to electronic tools, within terms that are certain and consistent with the rights of the data subjects. It remains the responsibility of the Data Controller to decide whether to independently make backup copies during the term of the agreement and for a 60-day period following its termination. *Logging* – The systems may be configured in such a manner as to track access requests and, where appropriate, other activities that are carried out, in relation to the different types of users (Administrator, Super User, etc.), and shall be protected by appropriate security measures ensuring their integrity. *Firewall, IDS/IPS* – The systems for preventing intrusions, such as Firewall and IDS/IPS shall be placed in the network segment connecting the cloud infrastructure with the internet in order to intercept any malicious activity aimed at debasing, in full or in part, the provision of the service. In the case at issue, the adopted equipment belongs to the type UTM SourceFire (Cisco), which includes both the Firewall and the IDS/IPS component. *Incident Management* – The Provider has adopted a specific Incident Management procedure aimed at ensuring restoration of the ordinary service operations at the soonest while ensuring to maintain best service levels. *High Reliability* – The Provider ensures high reliability in the following terms: • The Server Architecture shall be based on the VMWare virtualization solution and be implemented by creating physical and virtual redundancies of each system, in order to ensure fault-tolerance and removal of single points of failure. In particular, in case of system failure, the virtual environment managing software shall be able to reallocate current activities to other systems (principles of high availability and load balancing), minimizing service inefficiencies and ensuring persistence of existing connections.

	• Each Server is placed on a SAN connected via high-speed iSCSI. • All infrastructure components, including servers, security and network equipment, Storage systems and SAN infrastructure, have been duplicated in full, in order to eliminate each single point of failure. • The network infrastructure has been designed to protect front-end systems from the Internet and from internal networks using a DMZ shielded by means of two-layer separate firewalls (Defence-in-Depth strategy): a boundary firewall connected to the Internet and a second firewall, including Intrusion Prevention and antimalware features and belonging to the organization, setup to protect the DMZ and backend systems. *Data centre* – The virtualization environment (including the SAN – Storage Area Network) is placed on servers that are hosted in a data centre located in Italy and managed by a certified ISO 27001 provider. In particular, the following security measures shall be implemented to protect the Data Centre: • Exterior perimeter security: • External fence marking the boundary of the property not lower than 3 meters' height, equipped with passive anti climb protection • Monitoring of external areas by means of infrared barriers and/or video analysis systems and by video surveillance with recording systems • Restricted/individual pedestrian access • Restricted vehicle access • Armed patrols • Interior perimeter security: • Surveillance room for the control of internal and external areas, supervision • Use of alarms, management of visitors by delivering badges according to company policies and to specific regulations for data centres • Reception desk for entry control • Three-arm turnstiles placed opposite to the surveillance room and reception desk • High security inner perimeter: • Interlocked access to system rooms equipped with passive protection • Entry control system based on lists of "AUTHORIZED" people • Magnetic sensors detecting the state of doors • Emergency exits with sensors detecting the state of door All alarms are remotely linked to the surveillance room.

C – BUSINESS PROCESS OUTSOURCING (BPO)

Organizational Security Measures	*Certifications* – The Provider has obtained the following certifications/assessments: • ISO/IEC 27001:2013: "Delivery of services for the design and management of ICT infrastructure, management of applications within the Group and management of Cloud infrastructure (IaaS)". • ISO/IEC 27018:2014 for the protection of personal data in Public Cloud services. *User Policies and Regulations* – The Provider has adopted detailed policies and regulations, which all users having access to information systems must comply with, aimed at granting that users' behaviour is appropriate to ensure compliance with the principles of confidentiality, availability and integrity of data while using information resources. *Logical access authorization* – The Provider defines access profiles based on the least privilege necessary to carry out the assigned duties. The authorization profiles are selected and configured prior to the beginning of the processing and in such a manner that access will be restricted only to those data that are strictly necessary for the processing activities. The profiles undergo regular audits aimed at assessing whether the requirements to maintain the assigned profiles are still met. *Assistance interventions* – The Provider shall manage assistance interventions with the aim of ensuring that only contractual activities are performed and that any unnecessary processing in relation to Personal Data of the Client or of the Final User is prevented. *Change Management* – The Provider has implemented a specific procedure to regulate the Change Management process in view of the introduction (if any) of technological innovations or in case of modifications (if any) of its basic and organizational structure. *Data Protection Impact Assessment (DPIA)* – In compliance with Articles 35 and 36 of the GDPR and based on the document "WP248 – Guidelines on Data Protection Impact Assessment", adopted by the Article 29 Working Party, the Provider has prepared its own methodology for the analysis and assessments of those processing activities that, taking into account the nature, scope, context and purposes of the processing, are likely to result in a high risk for the rights and freedoms of natural persons, in order to be able to carry out an assessment of the impact on the protection of personal data prior to the processing.

	Incident Management – The Provider has adopted a specific Incident Management procedure aimed at ensuring restoration of the ordinary service operations at the soonest while ensuring to maintain best service levels. *Data Breach* – The Provider has implemented a special procedure, aimed at the management of events and incidents that are likely to have an impact on personal data, which defines the roles and responsibilities, the process for detection of the (suspected or actual) incident/breach, the implementation of remedial actions, the response to, and containment of, such incident/breach as well as the formalities to inform the Client of personal data breaches. *Training*: The Provider will periodically offer training courses on proper handling of personal data to members of its personnel that are involved in the processing activities.
Technical Security Measures	*High Reliability* – The Provider ensures high reliability in the following terms: • The Server Architecture shall be based on the VMWare virtualization solution and be implemented by creating physical and virtual redundancies of each system, in order to ensure fault-tolerance and removal of single points of failure. In particular, in case of system failure, the virtual environment managing software shall be able to reallocate current activities to other systems (principles of high availability and load balancing), minimizing service inefficiencies and ensuring persistence of existing connections. • Each Server is placed on a SAN connected via high-speed iSCSI. • All infrastructure components, including servers, security and network equipment, Storage systems and SAN infrastructure, have been duplicated in full, in order to eliminate each single point of failure. • The network infrastructure has been designed to protect front-end systems from the Internet and from internal networks using a DMZ shielded by means of two-layer separate firewalls (Defence-in-Depth strategy): a boundary firewall connected to the Internet and a second firewall, including Intrusion Prevention and antimalware features and belonging to the organization, setup to protect the DMZ and backend systems. *Hardening* – Specially designed hardening activities shall be implemented with the aim of preventing security incidents by minimizing the architectural weaknesses of the operating systems, of the applications and of network equipment by taking into due account, in particular, the reduction of the risks

	relating to system vulnerabilities, the reduction of the risks relating to the applications installed on the systems, and the increase of the protection level covering the services provided. *Firewall, IDS/IPS* – The systems for preventing intrusions, such as Firewall and IDS/IPS shall be placed in the network segment connecting the cloud infrastructure with the internet in order to intercept any malicious activity aimed at debasing, in full or in part, the provision of the service. In the case at issue, the adopted equipment belongs to the type UTM SourceFire (Cisco), which includes both the Firewall and the IDS/IPS component. *Security of communication lines* – Within the extent of its responsibilities the Provider shall implement secure communication protocols that are in line with the available technology. *Protection from malware* – The VMs shall be protected against the risk of an intrusion and of the activity of certain programs by activation of appropriate electronic tools to be periodically updated. All VMs shall be managed through antivirus features (at both hypervisor and infrastructure level). *Authentication Credentials* – The systems shall be configured in such a manner that access will be granted exclusively to those provided with authentication credentials allowing unique identification of the user. This include: a code associated to a confidential password that shall only be known by the user, or an authentication device that shall only be held and used by the user, which may, in certain cases, be associated with an ID code or a password. *Password* – The use of a password, as far as concerns its basic features, being the obligation to change it at the first access, the minimum length, the absence of elements that may be easily referred to its holder, the rules about its complexity, the expiration, history, assessment of strength in context, display and storage, will comply with the best practices. Users being provided with credentials shall also receive specific instructions concerning the measures that must be adopted to ensure that such credentials remain secret. *Logging* – The systems may be configured in such a manner as to track access requests and, where appropriate, other activities that are carried out, in relation to the different types of users (Administrator, Super User, etc.), and shall be protected by appropriate security measures ensuring their integrity.

	Backup & Restore – Appropriate measures shall be implemented aimed at ensuring restoration of access to data in case of damages to such data or to electronic tools, within terms that are certain and consistent with the rights of the data subjects. It remains the responsibility of the Data Controller to decide whether to independently make backup copies during the term of the agreement and for a 60-day period following its termination. If so required by any agreement, a continuity operation plan shall be implemented and, where necessary, integrated with the disaster recovery plan. These plans ensure the availability and access to the systems also in the event of serious adverse events that may persist in time. *Vulnerability Assessment & Penetration Test* – The Provider shall regularly carry out vulnerability analyses aimed at assessing the level of exposure to known vulnerabilities, in relation to both the infrastructures and the operations framework, taking into account either already operating systems and systems that are under development. When deemed appropriate, in relation to those potential risks that have been identified, the assessments above are complemented, from time to time, by special Penetration Test technics, simulating unauthorized access in various scenarios of attack, with the aim of controlling the level of security attained by applications/systems/networks by using the identified vulnerabilities to circumvent the physic/logic security mechanisms and gain access to them. The outcome of such assessments is thoroughly examined in order to detect and implement improvements that are necessary to ensure the high level of security that is required. *System Administrators* – All users operating as System Administrators shall be indicated in a list to be regularly updated and the duties assigned to them shall be duly defined in special documents of appointment. The activity performed by System Administrators shall be monitored by means of a log management system allowing to accurately trace all performed activities and to store such data in an immutable manner in order to allow the monitoring also after performance. The behaviour of System Administrators shall be audited to verify compliance with the organizational, technical and security measures in relation to the processing of personal data as required by current regulations. *Data centre* – The virtualization environment (including the SAN – Storage Area Network) is placed on servers that are hosted in a data centre located in Italy and managed by a certified ISO 27001 provider. In particular, the following security measures shall be implemented to protect the Data Centre: • Exterior perimeter security:

	• External fence marking the boundary of the property not lower than 3 meters' height, equipped with passive anti climb protection • Monitoring of external areas by means of infrared barriers and/or video analysis systems and by video surveillance with recording systems • Restricted/individual pedestrian access • Restricted vehicle access • Armed patrols • Interior perimeter security: • Surveillance room for the control of internal and external areas, supervision • Use of alarms, management of visitors by delivering badges according to company policies and to specific regulations for data centres • Reception desk for entry control • Three-arm turnstiles placed opposite to the surveillance room and reception desk • High security inner perimeter: • Interlocked access to system rooms equipped with passive protection • Entry control system based on lists of "AUTHORIZED" people • Magnetic sensors detecting the state of doors • Emergency exits with sensors detecting the state of door All alarms are remotely linked to the surveillance room.

D – BPI (BUSINESS PROCESS INSOURCING)

Organizational Security Measures	*User Policies and Regulations* – The Provider has adopted detailed policies and regulations, which all users having access to information systems must comply with, aimed at granting that users' behaviour is appropriate to ensure compliance with the principles of confidentiality, availability and integrity of data while using information resources. *Logical access authorization* – The Provider defines access profiles based on the least privilege necessary to carry out the assigned duties. The authorization profiles are selected and configured prior to the beginning of the processing and in such a manner that access will be restricted only to those data that are strictly necessary for the processing activities. The profiles undergo regular audits aimed at assessing whether the requirements to maintain the assigned profiles are still met. *Data Breach* – The Provider has implemented a special procedure, aimed at the management of events and incidents that are likely to have an impact on personal data, which defines the roles and responsibilities, the process for detection of the (suspected or actual) incident/breach, the implementation of remedial actions, the response to, and containment of, such incident/breach as well as the formalities to inform the Client of personal data breaches. *Training*: The Provider will periodically offer training courses on proper handling of personal data to members of its personnel that are involved in the processing activities.
Technical Security Measures	*Security of communication lines* – Within the extent of its responsibilities the Provider shall implement secure communication protocols that are in line with the available technology in relation to the authentication process. *Backup & Restore* – If so required by any agreement, appropriate measures shall be implemented aimed at ensuring restoration of access to data in case of damages to such data or to electronic tools, within terms that are certain and consistent with the rights of the data subjects.

E – ON PREMISES

Organizational Security Measures	*User Policies and Regulations* – The Provider has adopted detailed policies and regulations, which all users having access to information systems must comply with, aimed at granting that users' behaviour is appropriate to ensure compliance with the principles of confidentiality, availability and integrity of data while using information resources. *Logical access authorization* – The Provider defines access profiles based on the least privilege necessary to carry out the assigned duties. The authorization profiles are selected and configured prior to the beginning of the processing and in such a manner that access will be restricted only to those data that are strictly necessary for the processing activities. The profiles undergo regular audits aimed at assessing whether the requirements to maintain the assigned profiles are still met. *Assistance interventions* – The Provider shall manage assistance interventions with the aim of ensuring that only contractual activities are performed and that any unnecessary processing in relation to Personal Data of the Client is prevented. *Incident Management & Data Breach* – The Provider has implemented a special procedure, aimed at the management of events and incidents that are likely to have an impact on personal data, which defines the roles and responsibilities, the process for detection of the (suspected or actual) incident/breach, the implementation of remedial actions, the response to, and containment of, such incident/breach as well as the formalities to inform the Client of personal data breaches. *Training*: The Provider will periodically offer training courses on proper handling of personal data to members of its personnel that are involved in the processing activities.
Technical Security Measures	*Security of communication lines* – Within the extent of its responsibilities, during the technical assistance phase, the Provider shall implement secure communication protocols that are in line with the available technology. *Protection from malware* – Workstations used during the technical assistance phase shall be protected against the risk of an intrusion and of the activity of certain programs by activation of appropriate electronic tools to be periodically updated. All VMs are managed through antivirus features (at both hypervisor and infrastructure level).

	System Administrators – All users operating as System Administrators shall be indicated in a list to be regularly updated and the duties assigned to them shall be duly defined in special documents of appointment. The activity performed by System Administrators shall be monitored by means of a log management system allowing to accurately trace all performed activities and to store such data in an immutable manner in order to allow the monitoring also after performance. The behaviour of System Administrators shall be audited to verify compliance with the organizational, technical and security measures in relation to the processing of personal data as required by current regulations.