Data Processing Agreement

Diennea S.r.l., with registered office in Faenza (RA), Viale Marconi 30/14, P. IVA 02243600398 ("**Diennea**", hereinafter also "**Supplier**", or "**Processor**") and the signatory counterparty ("**Client**") have entered into a contract or another binding agreement for the provision of the Processor Services, or, again, have concluded negotiations with a view to stipulating a contract, involving the processing of personal data (hereinafter, as amended from time to time, only the "**Agreement**").

This Data Processing Agreement (including its annexes, "**Data Processing Agreement**") contains the provisions of Article 28 GDPR as interpreted by the European Data Protection Board in its Opinion 14/2019.

This Data Processing Agreement and the processing of data relating to the Supplier Services as described in Annex 1 prevail over any other previously applicable agreement between the parties.

This Data Processing Agreement is entered into by Diennea and the Client and supplements the Agreement. The Data Processing Agreement will be effective, and replace any other previously applicable agreement between the parties relating to the same subject matter (including any amendment or addendum to the processing of data relating to Processor Services), from the Effective Date and for the entire Period.

If you are entering into this Data Processing Agreement on behalf of the Client, you warrant that: (a) you have full legal authority to bind the Client to this Data Processing Agreement; and (b) you agree, on behalf of the Client, to this Data Processing Agreement. If you do not have the legal authority to bind the Client, please do not sign this Data Processing Agreement and pass it on to the relevant representative.

1. Preamble

The Data Processing Agreement reflects the parties' agreement on the processing of Client Personal Data as governed by European and National Legislation.

2. Definitions

2.1 All capitalised terms in the Data Processing Agreement have the following meanings:

"**Additional Instructions**" means the additional instructions set out in Annex 4.
"**EEA**" means the European Economic Area.
"**Effective Date**" means the date on which the Client signed, accepted or the parties have otherwise agreed to the effectiveness of the Agreement or the Data Processing Agreement.
"**European and National Legislation**" means the GDPR and the EU Member State legislation applicable to the processing of Client Personal Data.
"**Client Personal Data**" means the personal data that is processed by Diennea on behalf of the Client in the provision of the Processor Services by Diennea.
"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.
"**Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Client Personal Data on systems managed or otherwise controlled by Diennea.
"**Notification E-mail Address**" means in alternative succession, the email address: a) of Client's Data Protection Officer (if appointed); b) specified by the Client in the Agreement; c) used by the Client during the provision of the Processor Services to receive certain notifications from Diennea relating to this Data Processing Agreement.
"**Parties**" means the Client and Diennea.
"**Period**" means the period from the Effective Date until the termination of the provision by Diennea of the Processor's Services pursuant to the Agreement.
"**Processor Services**" means the services optioned in the Agreement and described collectively in Annex 1(B).
"**Security Documentation**" means any security certification or documentation (e.g., description of organizational and technical security measures, disaster recovery and business continuity plans, etc.) that Diennea makes available in relation to the Processor's Services. This definition includes the evidence referred to in Sections 7.4 (Security certification), 8 (Data protection impact assessments and prior consultation), 11.3.(a) and 12.2 (Supplier's contact details and record of processing), 17 (Insurance).
"**Security Measures**" has the meaning set out in Section 7.1.1 (Security Measures on Supplier's Systems).
"**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR, as approved by the European Parliament and the Council available here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en.
"**Subprocessors**" means the third parties authorised under this Data Processing Agreement to process Client Personal Data in order to provide – under Annex 3 – all or part of the Processor Services and/or any related technical support.
"**Subsidiary**" means a legal entity, which belongs to a corporate group, which directly or indirectly has control or is controlled by a party.
"**Supervisory Authority**" has the meaning as defined in the GDPR.
"**Transfer Mechanisms**" means a binding decision issued by the European Commission allowing the transfer of personal data from the EEA to a third country whose domestic law provides an adequate level of protection of personal data. Where such binding decision is not available or effective, this definition means the Standard Contractual Clauses, as well as binding corporate rules (BCRs) approved by a competent Supervisory Authority.

2.2 The terms "**Personal Data**", "**Data Subject**", "**Processor**", "**Controller**", and "**Processing**" have the meaning indicated in the GDPR. The terms "**Data Exporter**" and "**Data Importer**" have the meaning indicated in the Standard Contractual Clauses.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

2.3 The terms **'include'** and **'included'** means "including but not limited to". Any examples in the Data Processing Agreement are illustrative and are not the only examples of a particular concept.
2.4 Any reference to a law, regulation, statute or other legislative act is a reference to it, as amended or reformulated from time to time.
2.5 Any reference to a "**Clause**" refers to the clauses included in the Standard Contractual Clauses. Any reference to a "**Section**" refers to the sections of this Data Processing Agreement.
2.6 If this Data Processing Agreement is translated into another language and there is a discrepancy between the English text and the translated text, the English text shall prevail.

3. Period

This Data Processing Agreement shall be effective for the entire Period and until the Supplier deletes all Client Personal Data.

4. Scope of application

4.1 **Application of the Processor's Services**. This Data Processing Agreement applies only to the Processor Services for which the parties agreed to this Data Processing Agreement.
4.2 **Application of the Additional Instructions**. The Additional Instructions supplement this Data Processing Agreement.

5. Data processing

5.1 **Roles, responsibilities and instructions**
5.1.1 The parties acknowledge and agree that: (a) Annex 1 describes the subject matter and details of the processing of Client Personal Data; (b) Diennea acts as a Processor of Client Personal Data under European and National Legislation; (c) the Client acts as Controller or Processor, as applicable, of Client Personal Data under European and National Legislation; and (d) each party will comply with the obligations applicable to it under European and National Legislation with respect to Client Personal Data.
5.1.2 **Authorisation by the third Holder.** If the Client acts as Processor, the Client warrants to the Supplier that Client's instructions and actions in relation to Client Personal Data, including the appointment of Diennea, have been authorised by the respective Controller.
5.2 **Client instructions.** By entering into this Data Processing Agreement, the Client instructs Diennea to process Client Personal Data: (a) only in accordance with applicable law: (b) only to provide the Processor Services and any related technical support, without prejudice to the Processor's faculty to process it in anonymized and/or aggregate form for statistical purposes and to improve the Processor Services; (c) as further specified/indicated by the Client through its use of Processor Services (including changes to the settings and/or functionality of the Processor Services) and any related technical support; (d) as documented in the Agreement, including this Data Processing Agreement; and (e) as further documented in any written instruction provided by the Client to the Supplier as a further instruction for the purposes of this Data Processing Agreement.
5.3 **Supplier's compliance with the instructions**. The Supplier shall comply with the instructions described in Section 5.2 (Client Instructions) unless the European or National Legislation to which the Supplier is subject requires the Supplier to undertake a different or further processing of Client Personal Data (e.g., transfer of Personal Data to a third country or international organization), in which case the Supplier shall promptly inform the Client at the Notification E-mail Address (unless such legislation prohibits Diennea from doing so on important grounds of public interest). In no case is the Supplier under the obligation of performing a comprehensive legal examination with respect to a Client's written instruction.

6. Deletion and export of data

6.1 **Deletion and export for the Period**
6.1.1 Processor Services with export functionality. If the Processor Services include the possibility for the Client to export Client Personal Data autonomously and in interoperable format, the Supplier shall ensure that this operation is guaranteed for the entire Period, unless otherwise agreed with the Client in writing.
6.1.2 **Processor Services with deletion functionality**. If the Processor Services include the possibility for the Client to autonomously delete Client Personal Data, the Supplier shall ensure that such deletion from its systems is carried out as soon as reasonably possible, unless European and National Legislation requires further storage of the Client Personal Data to be deleted.
6.1.3 **Processor Services without deletion or extraction functionality.** During the Period, if Processor Services do not include the possibility for the Client to extract and/or delete Client Personal Data autonomously, the Supplier shall comply with any request by the Client to facilitate such operation in the same manner and timeframe indicated in Section 6.1.1 (Processor Services with export functionality) and Section 6.1.2 (Processor Services with deletion functionality).
6.1.4 The Data Processor may retain Client Personal Data which is stored in accordance with regular computer back-up operations in compliance with the Data Processor's (and/or Subprocessors') disaster recovery and business continuity protocols, provided that the Data Processor shall not, and shall not allow its Subprocessors to, actively or intentionally Process such Client Personal Data for any purpose other than the performance of the Processor Services.
6.2 **Deletion on Period expiry.** Without prejudice to the provisions of Section 6.1.1 (Processor Services with export functionality), upon expiration of the Period, the Client orders the Supplier to delete all Client Personal Data (including existing copies) from Supplier's systems in accordance with applicable law. The Supplier shall execute this instruction as soon as reasonably practicable, unless the European and National Legislation requires further storage of the Client Personal Data to be deleted and without prejudice to Section 6.1.4.

7. Data security

7.1 **Security measures and assistance by the Supplier**
7.1.1 **Security Measures on Supplier's systems**. The Supplier will adopt and maintain technical and organisational measures to protect Client Personal Data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access as described in Annex 2. Taking into account the state of the art and the costs of implementation, as well as the nature, scope, context and purpose of the processing carried out via the Processor Services, as well as the risk of varying likelihood and severity for the rights and

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

freedoms of natural persons, Annex 2 will include, where is the case, security measures: (a) to encrypt personal data; (b) to help ensure the ongoing confidentiality, integrity, availability and resilience of Supplier's systems and services; (c) to help restore timely personal data following an incident; and (d) to periodically verify effectiveness. The Supplier has the right to update or modify the Security Measures from time to time, provided that such updates and modifications do not lead to a degradation of the overall security of the Processor Services.

7.1.2 **Security Measures for Supplier's personnel.** The Supplier shall take appropriate measures to ensure compliance with the Security Measures by all those operating under its authority including its employees, agents, contractors and Subprocessors to the extent applicable to their scope of performance, including assuring that all persons authorised to process Client Personal Data have committed themselves to confidentiality or are subject to an appropriate statutory obligation of confidentiality in accordance with European and National Legislation.

7.1.3 **Supplier's security assistance**. Taking into account the nature of processing and the information available to the Supplier, Diennea will assist the Client in ensuring compliance with eventual obligations of the Client regarding security of personal data and personal data breaches, including (if applicable) Client's obligations under Articles 32 to 34 GDPR, through:

(a) the implementation and maintenance of Security Measures in accordance with Section 7.1.1. (Security Measures on Supplier's systems);

(b) the implementation of the provisions of Section 7.2 (Incidents); and

(c) providing the Client with the Security Documentation in accordance with Section 7.5.1 (Review of Security Documentation) and the information provided for in this Data Processing Agreement.

7.2 **Incidents**

7.2.1 **Incident notification**. If the Supplier becomes aware of an Incident, Diennea shall: (a) inform the Client of the Incident without undue delay; and (b) take reasonable measures to minimise the harm and secure Client Personal Data in a timely manner.

7.2.2 **Incident details**. Notifications made pursuant to Section 7.2.1 (Incident Notification) shall describe to the maximum extent possible the details of the Incident, including the measures that Diennea has taken or recommends the Client to take to address the Incident and mitigate its effects.

7.2.3 **Delivery of Incident notification**. The Supplier will deliver its notification of any Incident to the Notification E-mail Address or, at Diennea discretion, by other direct communications (e.g., by telephone call or face-to-face meeting). The Client is solely responsible for ensuring that the Notification E-mail Address is up-to-date, accurate and monitored.

7.2.4 **Third-party notification**. The Client is the sole party responsible for compliance with the obligations concerning the notification of Incidents applicable to the Client and the fulfilment of any obligation to notify/inform third parties of such Incidents.

7.2.5 **Value of the notification**. Diennea's notification of or response to an Incident within the meaning of this Section 7.2 (Incidents) shall not be construed as an acknowledgment by Diennea of any fault or liability in connection with the Incident.

7.3 **Client's security responsibility and assessment**

7.3.1 **Client's security responsibility**. Without prejudice to Supplier's obligations under Sections 7.1 (Security Measures and Assistance by Diennea) and 7.2 (Incidents), the Client agrees that:

(a) the Client is solely responsible for its use of the Processor Services, including:

i. the appropriate use of the Processor Services to ensure a level of risk security adequate for the Client Personal Data, and

ii. protecting authentication credentials, systems and devices used by the Client to access the Processor Services; and

(b) Diennea has no obligation to protect Client Personal Data that the Client chooses to store or transfer outside the Supplier's and/or Subprocessor's systems.

7.3.2 **Client's security assessment.** The Client acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing Client Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons) Diennea Security Measures as indicated in Section 7.1.1 (Security Measures on Supplier's systems) provide a level of security adequate to the risk deriving from the processing of Client Personal Data.

7.4 **Security certification**. To evaluate and help ensure the continued effectiveness of the Security Measures, Diennea may, at its sole discretion, supplement the Security Measures and Security Documentation by implementing certifications (e.g., ISO27001), codes of conduct and/or certification mechanisms.

7.5 **Checks and audits**

7.5.1 **Review of Security Documentation**. In order to demonstrate Diennea's compliance with its obligations under this Data Processing Agreement, Diennea will make the Security Documentation available to the Client.

7.5.2 **Client's audit rights**. The parties agree that:

(a) the Supplier will allow the Client or a third-party auditor appointed by the Client to carry out audits to verify Supplier's compliance with its obligations under this Data Processing Agreement in accordance with Section 7.5.3 (Additional conditions for audits). The Supplier will contribute to such audits in accordance with this Section 7.5 (Checks and Audits).

(b) the Client may also conduct an audit to verify Supplier's compliance with its obligations under this Data Processing Agreement by reviewing the certificates issued pursuant to Section 7.4 (Security certification), which reflect the outcome of an audit conducted by a third-party auditor.

7.5.3 **Additional conditions for audits**. Regarding audit, the parties agree that:

(a) the Client will send the Supplier any request for an audit in accordance with Section 7.5.2(a) to the following e-mail address: audit@diennea.com;

(b) upon receipt by the Supplier of a request pursuant to Section 7.5.3(a), the Client and the Supplier undertake to discuss and agree in advance on the identity of the auditor, the start date – which in any case cannot be identified earlier than twenty (20) working days from the date on which the Supplier receives the audit request from the Client –, scope and duration, security and confidentiality controls applicable to, any audit pursuant to Section 7.5.2(a);

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

c) the Client acknowledges and accepts that the costs incurred by the Client for the audit activities are at its own exclusive charge; the Client has to faculty to conduct an audit of the Supplier, without cost, of a duration of one (1) working day, within any given solar year, without prejudice to the Supplier's right to charge the Client with the costs of any further audit activities not foreseen under this article;
(d) the Supplier may object to any third-party auditor appointed by the Client to carry out audits pursuant to Section 7.5.2(a) if, under reasonable discretion of Diennea, it is not suitably qualified or independent; it is a competitor of Diennea; it is manifestly unsuitable to the activity. Any objection of this type by Diennea will require the Client to appoint another auditor or to conduct the audit itself;
(e) the Client is informed and accepts that the audit activities must give due consideration to the rules regarding security and/or confidentiality, which may impose limits to the scope of the audit. In particular, nothing in this Data Processing Agreement will require the Supplier to disclose or grant access to the Client or its third-party auditor to:

(i) any data of any other client of the Supplier;
(ii) any of Supplier's internal accounting or financial information;
(iii) any trade secret and know-how of the Supplier;
(iv) any information that could compromise the security of Diennea's systems or premises; or cause Diennea to breach its obligations under European and National Legislation or its security obligations towards the Client or third parties; or
(v) any information to which the Client or its third-party auditor seeks access for reasons other than good faith fulfilment of the Client's obligations under European and National Legislation.

(f) the performance of audits shall be subject to a specific confidentiality agreement between all parties involved.

8. Data protection impact assessments and prior consultation

8.1 Upon request of the Client made with sufficient advance notice, Diennea agrees (taking into account the nature of the processing and the information available to Diennea) to assist the Client in ensuring compliance with any obligations of the Client regarding data protection impact assessments and prior consultation, including (where applicable) the Client's obligations under Articles 35 and 36 GDPR, by: (a) the provision of Security Documentation in accordance with Section 7.5.1 (Review of Security Documentation); (b) the provision of information contained in this Data Processing Agreement; and (c) the provision or making available, in compliance with Diennea's standard practices, of other materials relating to the Processor Services and/or the processing of Client Personal Data (e.g., support materials).

9. Data Subjects rights

9.1 **Responses to Data Subjects requests**. If the Supplier receives a request from a Data Subject in relation to Client Personal Data, the Supplier will respond to the request inviting the Data Subject to submit his/her request to the Notification E-mail Address (or, if opportune and/or possible, the Supplier will directly inform the Client of the request and forward the Notification E-mail Address to the latter) so that the Client may provide a response to the Data Subject's request.
9.2 **Supplier's Data Subject request assistance**. The Client accepts that Diennea (taking into account the nature of the processing of Client Personal Data) will assist the Client in the fulfilment of any of the Client's obligations with respect to Data Subjects' requests for the exercise of their rights as set forth in Chapter III GDPR, by: (a) if applicable, the provision of specific functionalities in the Processor Services; (b) complying with the commitments set out in Section 9.1 (Responses to Data Subjects requests). The Client acknowledges and agrees that in the event that such cooperation and assistance require significant use of resources by the Supplier and the Client is able to acquire such information on its own, such effort will be chargeable, upon notice and agreement, to the Client.

10. Data transfers

10.1 **Data storage and processing facilities.** The Client agrees and authorizes the Supplier to process (also by means of Subprocessors) Client Personal Data inside and outside the EEA, provided that such processing is supported by appropriate Transfer Mechanisms, to be provided in Annex 3.
10.2 **Subprocessor Transfer Mechanism**. Where the Supplier intends to make use of one or more subprocessors established outside the EEA and no transfer mechanisms are available other than the Standard Contractual Clauses, the Parties agree that: i) the Supplier and its subprocessor(s) shall be considered "parties" pursuant to "MODULE THREE: transfer processor to processor" of the Standard Contractual Clauses; ii) Annexes I-IV of this DPA shall replace or be substantially reflected in the annexes to the Standard Contractual Clauses.

11. Subprocessors

11.1 **Authorisation to Subprocessor engagement**. The Client grants a general authorization for the engagement of Subprocessors for the provision of the Processor Services.
11.2 **Information about Subprocessors.** The list and the respective information on Subprocessors are available in Annex 3 of this Data Processing Agreement.
11.3 **Requirements for Subprocessors engagement**. When engaging a Subprocessor, the Supplier will:
(a) ensure via a written contract or other binding legal act that:

(i) the Subprocessor only accesses and uses Client Personal Data to the extent necessary to perform the obligations subcontracted to it in accordance with the Agreement (including this Data Processing Agreement) and the Transfer Mechanisms;
(ii) the same data protection obligations as set forth in Article 28(3) GDPR as well as the main obligations of this Data Processing Agreement (or in any case obligations which offer guarantees not less than those offered by the Supplier) are imposed on the Subprocessor.

(b) remain fully responsible for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.
11.4 **Possibility to object to change of Subprocessors.** The parties agree that:

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

(a) during the Period, the Supplier shall notify the Client at the Notification E-mail Address of its intention to engage new Subprocessors for the processing of Client Personal Data, such that failure of the Client to present objection – within 10 days of the above notification – shall be understood as (tacit) consent to the engagement of each Subprocessor. Such communication will include the name, the activity carried out, the country of establishment of Subprocessors;
(b) in the event of Client's objection to any of the new Subprocessors, the parties shall cooperate in good faith to find appropriate solutions to allow the continuation of the Agreement and, if this is not possible, each party shall have the right to request the termination of the Agreement to be communicated to the other party within 30 days of Client's objection to the engagement of the new Subprocessors as described in Section 11.4(a).

12. Supplier's contacts details and record of processing

12.1 **Supplier contacts details.** The Client will contact Diennea in relation to everything contained in this Data Processing Agreement, at the following e-mail address: dpo@diennea.com.
12.2 **Record of processing**. The Client acknowledges that Diennea is required under the GDPR to: (a) collect and store certain information, including the name and contact details of each Processor and Controller involved in the processing of Client Personal Data and (if appointed) the representative and the data protection officer; and (b) make such information available to any Supervisory Authority. Consequently, the Client will provide such information to Diennea through the Notification E-mail Address indicated in Section 12.1 or any other means indicated by Diennea, and undertakes to ensure that all the information provided is always accurate and up to date.

13. Conflicts

13.1 **Conflicts between the parties' agreements**. In the event of any conflict or inconsistency between the provisions of the Agreement, the Data Processing Agreement and the Additional Instructions, the following order of precedence shall apply: (a) the Additional Instructions; (b) the remaining provisions of the Data Processing Agreement; and (c) the remaining provisions of the Agreement. Subject to any amendments to the Data Processing Agreement, the Agreement remains in full force and effect.
13.2 **Infringements of laws or regulations**. Any provision of the Agreement, the Data Processing Agreement and/or the Additional Instructions that is contrary to European and National Legislation shall be deemed not to be reproduced herein and shall be replaced in its entirety by the provision that has been violated if it cannot be derogated from by an agreement between the parties.

14. Modifications

14.1 **Changes to the Annexes**. From time to time, the Supplier may modify the content of the Annexes if expressly permitted by the Data Processing Agreement. The Supplier may amend the list of Processor Services in Annex 1 only: a) to reflect a change in the name of a service; b) to add a new service; or c) to delete a service in case: (i) all contracts for the provision of that service are terminated; or (ii) the Supplier has received the Client's consent.
14.2 **Amendments to the Data Processing Agreement**. Diennea may amend this Data Processing Agreement if the amendment:
(a) is expressly permitted by the Data Processing Agreement;
(b) is mandatory to comply with the applicable law, a judgment or other order of a court or guidelines issued by a Supervisory Authority or governmental authority;
(c) does not diminish the overall security of the Processor Services;
(d) does not extend the scope of application of (or eliminates any restrictions to) Diennea's right to process the data within the scope of the Additional Instructions or to process Client Personal Data as established under Section 5.3 (Diennea's compliance with the instructions);
(e) has no other negative impact on the rights of the Client pursuant to this Data Processing Agreement, as reasonably ascertained by Diennea.
14.3 **Notification of changes**. Except in the case indicated in Section 14.2(b) in which the amendment is immediately effective between the parties, if Diennea intends to amend this Data Processing Agreement pursuant to Section 14.2, Diennea will inform the Client at least 30 days before the amendment becomes effective (or in shorter period as may be required to comply with applicable law) by sending an e-mail to the Notification E-mail Address of the Client. If the Client opposes to such changes, the parties undertake to collaborate in good faith to find suitable solutions to allow the continuation of the Agreement and, where this is not possible, each party may withdraw from the Agreement by giving written notice to the other party within 30 days of Diennea's notification of the change; if none of the parties exercise the right to withdraw within the aforesaid term, the change is binding between the parties for all legal and contractual purposes.

15. Liability and compensation

15.1 **Perimeter of damages.** The parties acknowledge and accept that if a Data Subject complains ("**Claimant**"), against the parties, that it has suffered damage - material or immaterial - caused by a violation of European and National Legislation:
(a) the Party directly liable for the violation, pursuant to art. 82(2) GDPR, shall be fully liable for the material or immaterial damage caused to the Data Subject declaring from now on to indemnify and hold the other Party harmless, if it has not complied with the obligations of European and National Legislation specifically addressed to this Party;
(b) if the Supplier and the Client are involved in the same processing and are both liable for the damage caused to the Claimant, pursuant to paragraphs 2 and 3 of art. 82 GDPR, each of the two shall be jointly and severally liable for the entire amount of the damage, without prejudice, for both, to the right of recourse against the other for the share of compensation due to the same party based on the damage caused, as defined in Section 16.2 (Negotiation);
(c) if the damage caused to the Claimant is due to the violation of the provisions of this Data Processing Agreement or of the European and National Legislation and is entirely attributable to the Supplier, the Supplier shall be obliged to compensate the Client in full, if the latter has provided compensation for the Claimant in whole or in part;
(d) each Party shall indemnify or compensate the other party if and to the extent that it has contributed to the damage claimed by the Claimant or has failed to take appropriate mitigating measures, or has violated the provisions of this Data Processing Agreement or the European and National Legislation.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

15.2 **Negotiation.** In the case referred to in Section 16.1(b), the extent of the indemnity or compensation will be determined jointly by the parties by means of an agreement negotiated in good faith according to the portion of liability and the extent of the damage caused.

15.3 **Jurisdiction**. Without prejudice to the appointment of the Arbitrator, in the event of disputes relating to the execution or interpretation of this Data Processing Agreement, the parties hereby assign exclusive jurisdiction to the forum already identified in the Agreement, expressly derogating from any other provisions of international laws or conventions.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

Annex 1

A. *List Of Parties*

Controller: means the Client as defined in the Agreement

Processor

1. **Name**: Diennea S.r.l.
   Address: Viale G. Marconi n. 30/14 – 48018 Faenza (RA)
   DPO name: ICTLC S.P.A.
   DPO contact details: dpo@diennea.com

B. *Description Of Processing*

Nature and purposes of the processing
The Supplier will process Client Personal Data in order to provide the Processor Services, as defined in the Agreement signed between the Client and the Supplier, in accordance with the instructions contained in the Data Processing Agreement.
Depending to the Processor Services under the Agreement, Client Personal Data may include the following Personal Data:

Types of Data Subjects	☐Job applicants ☐Customers ☐Prospective customers ☐External Consultants/Collaborators ☐Contractors ☐Employees ☐Employees of contractors ☐Former Employees ☐Former Executives ☐Family members ☐Suppliers ☐Administered workers ☐Lawyers ☐Minors ☐Participants at events ☐Trainers/trainees ☐Visitors ☐ Subjects whose Personal Data are processed by the Client in the context of the use of the Processor Services
Personal Data processed	☐Data collected by tracking technologies and devices ☐Common identification data (e.g., first name, last name, address) ☐Data on life habits, consumption and behaviour ☐Data on family members/family status ☐Picture, video, sound ☐Fiscal code ☐ Additional categories of Personal Data processed by the Client through the Processor Services

Frequency of the Processing
Throughout the entire duration of the Agreement.

Duration of the processing
During the Period plus the period until all Client Personal Data are deleted by the Supplier in accordance with the Data Processing Agreement.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

Subject-matter, nature and duration of the processing performed by Subprocessors

Please refer to Annex 3 (Annex III of the Standard Contractual Clauses) for further information on this.

C. *Competent Supervisory Authority*

Autorità Garante per la protezione dei dati personali (Supervisory Authority of Italy).

The Parties may update the list of the types of Personal Data processed in the provision of the Processor Services, as required.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

Annex 2: Security Measures

Description of the technical and organisational measures

The Data Processor and the Subprocessors undertake to maintain no less than the technical and organisational measures described below.

Information security policies

Management direction for information security

Management should define a set of policies to clarify their direction of, and support for, information security. At the top level, there should be an overall "information security policy" as specified in ISO/IEC 27001 section 5.2.

Organization of information security

Internal organization

The organization should lay out the roles and responsibilities for information security and allocate them to individuals. Where relevant, duties should be segregated across roles and individuals to avoid conflicts of interest and prevent inappropriate activities.

Mobile devices and teleworking

There should be security policies and controls for mobile devices (such as laptops, tablet PCs, wearable ICT devices, smartphones, USB gadgets and other Boys' Toys) and teleworking (such as telecommuting, working-from home, road-warriors, and remote/virtual workplaces).

Human resource security

Prior to employment

Information security responsibilities should be taken into account when recruiting permanent employees, contractors and temporary staff (e.g. through adequate job descriptions, pre-employment screening) and included in contracts (e.g. terms and conditions of employment and other signed agreements defining security roles and responsibilities, compliance obligations etc.).

During employment

Managers should ensure that employees and contractors are made aware of and motivated to comply with their information security obligations. A formal disciplinary process is necessary to handle information security incidents allegedly caused by workers.

Termination and change of employment

Security aspects of a person's departure from the organization, or significant changes of roles within it, should be managed, such as returning corporate information and equipment in their possession, updating their access rights, and reminding them of their ongoing obligations under privacy and intellectual property laws, contractual terms etc. plus ethical expectations.

Asset management

Responsibility for assets

All information assets should be inventoried and owners should be identified to be held accountable for their security. 'Acceptable use' policies should be defined and assets should be returned when people leave the organization.

Information classification

Information should be classified and labelled by its owners according to the security protection needed, and handled appropriately.

Media handling

Information storage media should be managed, controlled, moved and disposed of in such a way that the information content is not compromised.

Access control

Business requirements of access control

The organization's requirements to control access to information assets should be clearly documented in an access control policy and procedures. Network access and connections should be restricted.

User access management

The allocation of access rights to users should be controlled from initial user registration through to removal of access rights when no longer required, including special restrictions for privileged access rights and the management of passwords (now called "secret authentication information") and regular reviews and updates of access rights should take place.

User responsibilities

Users should be made aware of their responsibilities towards maintaining effective access controls e.g. choosing strong passwords and keeping them confidential.

System and application access control

Information access should be restricted in accordance with the access control policy e.g. through secure log-on, password

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

management, control over privileged utilities and restricted access to program source code.

Cryptography

Cryptographic controls

There should be a policy on the use of encryption, plus cryptographic authentication and integrity controls such as digital signatures and message authentication codes, and cryptographic key management.

Physical and environmental security

Secure areas

Defined physical perimeters and barriers, with physical entry controls and working procedures, should protect the premises, offices, rooms, delivery/loading areas etc. against unauthorized access. Specialist advice should be sought regarding protection against fires, floods, earthquakes, bombs, etc.

Equipment

"Equipment" (meaning ICT equipment, mostly) plus supporting utilities (such as power and air conditioning) and cabling should be secured and maintained. Equipment and information should not be taken off-site unless authorized, and must be adequately protected both on and off-site. Information must be destroyed prior to storage media being disposed of or re-used. Unattended equipment must be secured and there should be a clear desk and clear screen policy.

Operations security

Operational procedures and responsibilities

IT operating responsibilities and procedures should be documented. Changes to IT facilities and systems should be controlled. Capacity and performance should be managed. Development, test and operational systems should be separated.

Protection from malware

Malware controls are required, including user awareness.

Backup

Appropriate backups should be taken and retained in accordance with a backup policy.

Logging and monitoring

System user and administrator/operator activities, exceptions, faults and information security events should be logged and protected. Clocks should be synchronized.

Control of operational software

Software installation on operational systems should be controlled.

Technical vulnerability management

Technical vulnerabilities should be patched, and there should be rules in place governing software installation by users.

Information systems audit considerations

IT audits should be planned and controlled to minimize adverse effects on production systems, or inappropriate data access.

Communications security

Network security management

Networks and network services should be secured, for example by segregation.

Information transfer

There should be policies, procedures and agreements (e.g. non-disclosure agreements) concerning information transfer to/from third parties, including electronic messaging.

System acquisition, development and maintenance

Security requirements of information systems

Security control requirements should be analysed and specified, including web applications and transactions.

Security in development and support processes

Rules governing secure software/systems development should be defined as policy. Changes to systems (both applications and operating systems) should be controlled. Software packages should ideally not be modified, and secure system engineering principles should be followed. The development environment should be secured, and outsourced development should be controlled. System security should be tested and acceptance criteria defined to include security aspects.

Test data

Test data should be carefully selected/generated and controlled.

Supplier relationships

Information security in supplier relationships

There should be policies, procedures, awareness etc. to protect the organization's information that is accessible to IT outsourcers and other external suppliers throughout the supply chain, agreed within the contracts or agreements.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

Supplier service delivery management

Service delivery by external suppliers should be monitored and reviewed/audited against the contracts/agreements. Service changes should be controlled.

Information security incident management

Management of information security incidents and improvements

There should be responsibilities and procedures to manage (report, assess, respond to and learn from) information security events, incidents and weaknesses consistently and effectively and in order to collect forensic evidence.

Information security aspects of business continuity management

Information security continuity

The continuity of information security should be planned, implemented and reviewed as an integral part of the organization's business continuity management systems.

Redundancies

IT facilities should have sufficient redundancy to satisfy availability requirements.

Compliance

Compliance with legal and contractual requirements

The organization must identify and document its obligations to external authorities and other third parties in relation to information security, including intellectual property, [business] records, privacy/personally identifiable information and cryptography.

Information security reviews

The organization's information security arrangements should be independently reviewed (audited) and reported to management. Managers should also routinely review employee and system compliance with security policies, procedures, etc. and initiate corrective actions where necessary.

With reference to the service MagNews SaaS and pursuant to Annex B of the Italian Privacy Code (Legislative Decree No. 196/2003) previously in force and to art. 32 of the GDPR, the Data Processor adopted - inter alia - the following security measures:

- implementation of an authentication system which assigns personal and confidential credentials based on identification code and password to each user;
- in MagNews it is possible to enable 2FA authentication and IP address blocking rules, such that user access to the platform back-end, web, FTP and Simply SMTP services is limited solely to specific IP addresses.
- the password meets the following requirements:
  (a) it must be composed of at least 8 characters (the size can be configured up to a maximum of 50 characters);
  (b) must not contain the username, and cannot be contained in the username;
  (c) must contain at least one lowercase letter;
  (d) must contain at least one capital letter;
  (e) must contain at least one number;
  (f) must contain at least one special character between: (_, -, $, £,%, #, &,!,?, ^, +, *) and has a configured 90-day expiration date;
- if password recovery is needed, the user receives an e-mail containing a temporary password that can only be used upon the first access to the Platform's web interface (so-called "one time password"). Diennea's Staff is not able to recover the password, but only to reset it. When the user logs in with the temporary password, a mask is shown to the user in which he or she shall enter and subsequently confirm a new password, which cannot be identical to the previous one;
- passwords are transmitted on an encrypted channel with SSL protocol and stored encrypted with strong encryption algorithm (AES256) within a specific table;
- implementation of an authorization system that, through a system of profiles, allows each Authorized Person, or homogeneous classes of Authorized Persons, to be able to process data compatibly with the task performed and the role covered according to the general principles of lawfulness, correctness, relevance and data minimization;
- all access interfaces and application pages are made safe through the use of secure protocols (HTTPS);
- Diennea guarantees the protection in case of data loss and corruption, along with a daily backup policy which involves copying data and configurations onto two different data centres and storing backup copies for 60 days. In addition, a disaster recovery system was implemented between two different data centres (geographically located approximately 400 km from each other) to ensure the continuity of the service and data. All backup and disaster recovery operations are governed by the business continuity plan (BCP). All data stored or "at rest", such as backup copies and disaster recovery, are stored in an encrypted (with strong AES256 algorithm) and protected;
- all servers hosting the service and all the electronic devices used by Diennea personnel are protected against any attempted intrusion and/or cyber attack by firewall, antivirus and DLP systems, IDS and HIDS systems and are subject to continuous updating and hardening (according to the CIS guidelines). In the case of use of removable and mobile devices these are encrypted (full disk encryption) to mitigate the risks of involuntary loss or theft;
- all Diennea systems are monitored 24/7 against attack threats and abnormal behaviour and all system administrators' accesses are traced and stored in an encrypted and non-modifiable manner in compliance with the current legislation;
- the service is provided by systems hosted by **the TIM S.p.A. data centers of Rozzano (MI) and Acilia (RM)**. Both of these structures are certified ISO 9001: 2015 and ISO /

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

IEC 27001: 2013 and guarantee the highest standards of physical and logical resilience and manage the physical security of access 24/7 through dedicated personnel and automatic detection and anti-intrusion systems: only expressly authorized personnel can directly access Diennea's systems;

- a continuous training and updating program has been planned for Diennea personnel on IT security and personal data protection issues;
- Diennea adopted a series of internal company policies disclosed to its staff, which undertook to guarantee the confidentiality and security of Diennea's customers' data;
- Diennea adopted and applies policies and procedures such as, for example:
    - rules for the use and exchange of data between the company's personnel from and to the customer;
    - rules for the management of electronic devices;
    - rules for managing the conclusion of the employment contract with the employees;
    - periodic check of the validity of the permits of the company users;
    - Change Control Management Policy;
    - Courtesy Security Notification Policy;
    - Incident Response and Notification Policy;
    - Data Breach Response and Notification Policy;
    - Development and Release Workflow Process.
- Diennea periodically performs (at least annually) risk assessment, vulnerability assessment and penetration testing and privacy audit activities in order to verify the level of security and maturity of its technological infrastructure and the procedures adopted, as well as the level of training of its personnel.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

Annex 3: List of Subprocessors

Annex 3, containing the list of Subprocessors employed by the Supplier, is available in the following ways:

- at the link https://www.diennea.com/en/list-of-sub-processors/;
- by written request to the e-mail address dpo@diennea.com.

In the event of any changes to the list shared at the time of signing this Data Processing Agreement, the Supplier shall send a notice to the Notification E-mail Address; from the Supplier's notification, the objection period referred to in Section 11.4(a) of the Data Processing Agreement above shall commence, it being understood that it is the Client's responsibility to consult the updated list in the manner referred to above.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

Annex 4 – Additional Instructions

The following Additional Instructions supplement this Data Processing Agreement:

1. *Instructions for System Administrators - version 1.0;*
   - The Supplier undertakes to comply with the provision of the Supervisory Authority called "*Measures and arrangements applying to the controllers of processing operations performed with the help of electronic tools in view of committing the task of system administrator*" (and its subsequent amendments).
   - The Supplier undertakes to proceed with the drafting of an individual designation letter for each system administrator, following the evaluation of the experience, capacity and reliability of the subjects, containing an analytical list of the areas of operation.
   - The Supplier undertakes to carry out, at least once a year, a process of review of the work of the system administrators through the means they deem appropriate.
   - The Supplier undertakes to produce, at Client's request, a list of the personnel designated as system administrators with a list of the functions assigned to them.
   - The Supplier undertakes to implement software that produces access logs relating to the systems on which the system administrators operate, with characteristics of completeness and inalterability as well as being subject to integrity verification and to be kept for at least six months.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com