**ANNEX TO THE LICENCE CONDITIONS OF USE OF THE REDHAB PLATFORM**
**DATA PROCESSING AGREEMENT ('DPA')**

WHEREAS

- by virtue of the Terms of Use of the RedHab Platform signed between RedAbissi S.r.l. and the Customer ("Main Agreement") for the use of the RedHab Platform, RedAbissi may come into contact with information which, in the context of the Customer's organisation, consists of personal data relating to interested parties operating under the authority of the Customer (the "Users");
- In relation to such data, therefore, the Customer is the data controller, while RedAbissi is the data processor, and as such are respectively defined in the Data Processing Agreement ("DPA");
- Article 4 (8) of the General Data Protection Regulation (EU) 2016/679 ("GDPR") defines "Data Processor" as the "natural or legal person, public authority, service or other body that processes personal data on behalf of the Data Controller";
- Article 28 (1) provides that "where a processing operation is to be carried out on behalf of a controller, the controller shall have recourse only to data processors providing sufficient guarantees to implement appropriate technical and organisational measures to ensure that the processing meets the requirements of this Regulation and to ensure the protection of the rights of the data subject";
- Article 28 (3) specifies that processing by a controller must be governed by "a contract or other legal act in accordance with Union or Member State law binding the controller to the processor and stipulating the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, the obligations and the rights of the data controller";
- the Annexes form an integral and substantial part of the DPA.

In view of the foregoing, the Parties agree as follows.

**1. Statements by the Parties**

1.1. The Data Controller, in the light of the verifications carried out, acknowledges that the Data Processor possesses the experience, capacity and reliability to ensure compliance with the provisions on Processing, including the security profile, and in any event to be able to provide sufficient guarantees to put in place adequate technical and organisational measures so that the Processing meets the requirements of the Privacy Law and guarantees the protection of the rights of the Data Subject.

1.2. The Controller expressly declares:

a. that it has chosen the person in charge in view of the above;
b. to authorise the Data Processor to process personal data either directly or with the help of the other Data Processors listed in Appendix C;
c. to be aware that the essential requisite for taking advantage of the services contractually agreed upon with RedAbissi is compliance with the fundamental principles of Data Processing as per Art. 5 GDPR insofar as the Data Controller is concerned, as well as the existence of a legal basis that determines the lawfulness of the processing of Personal Data, pursuant to Art. 6,
d. 7 and 9 of Regulation (EU) 2016/679;
e. that he/she is aware of his/her own responsibilities in relation to his/her role as the organisation that determines the means and purposes of the Processing, including (by way of example but not limited to) the correct configuration and use of the security functions controlled by him/her, also taking into account the limited possibility for RedAbissi to intervene in the configuration of the IT infrastructure in use at the Customer's premises;
f. to be in possession (where due) of all necessary authorisations from the Data Subjects to be able to process the Data, either independently or through RedAbissi.

**2. Subject of the Agreement**

2.1. The DPA governs the instructions that the Controller gives to the Processor for the purposes of the Processing, as well as the terms, conditions and reciprocal rights, obligations and responsibilities.

**3. Characteristics of Processing, Categories of Data and Data Subjects, Processing Instructions**

3.1. The Processing covered by the RedHab Platform Licence Conditions has the characteristics set out in Appendix A.

3.2. The Processor shall process the data indicated in Appendix A, in relation to each service. The Owner has the right to inform the Processor which of the information indicated in Appendix A for each Service he or she does not intend to collect; to this end, he or she undertakes to send a written communication to RedAbissi.

**4. Controller's rights**

4.1. The Controller has the right to:

a) supervise the work of the Processor, at their own cost;

b) object to changes (in addition to and/or replacement with respect to Appendix C) to the list of other Processors for the performance of specific processing activities on behalf of the Controller, within seven days of notification by RedAbissi;

c) give notice of the termination and/or suspension of the processing if this is required by the need to comply with prohibitions or obligations arising from the privacy law or applicable legislation, and/or measures/orders the Control Authority or other Authority;

d) recourse, against the Data Processor, of the amount. if any, paid by way of compensation for the damage suffered by the Data Subject, corresponding to the part of the liability of the Data Processor.

**5. Obligations of the Controller**

5.1. The Controller is obliged to:

a) send a written notice to RedAbissi in the event that it does not intend to collect, through the Services, any of the information among those listed in Appendix A for each service;

b) carry out the Processing in compliance with the privacy legislation and further applicable legislation, in particular to: - make information available to Data Subjects on the processing of personal data in accordance with Articles 13 and 14 GDPR; - collect (to the extent that it is due) consent to the processing of data from Data Subjects;

c) guarantee them the possibility of exercising their rights under Articles 15 to 22 of the GDPR;

d) indicate to the Processor the persons he appoints for audit and inspection activities, with at least thirty days' notice, communicating in the same terms the qualifications and competences of such persons in order to be able to assess possible conflicts of interest;

e) carry out (and/or have carried out) the activities referred to in the preceding point without interfering with the ordinary activities of the Processor;

f) forward to the Processor, without undue delay, any request from the Interested Parties involving his or her cooperation;

g) make any necessary communication to the Control Authority at the time of Termination;

h) promptly notify the Data Processor of the occurrence of technical problems concerning the Processing and the related security measures, which may entail the risk of destruction or loss, even accidental, of the Data, or of unauthorised access or processing that is not permitted or does not comply with the purposes;

i) express any opposition to the employment by the Processor of one or more of the persons listed in Appendix C, by means of a reasoned communication to be sent to the Processor no later than ten days after the signature of the DPA;

j) pay first any sums claimed for compensation by the Interested Parties from the Processor, without prejudice to the right of recourse against the latter following the ascertainment, in a final judgment, of its share of liability, if any.

**6. Rights of the data Processor**

6.1. The Processor has the right to:

a) receive adequate notice (of at least thirty days, except for reasons of justified and documented urgency) from the Controller regarding the performance by the latter of audits, auditing and/or inspection activities, as well as to know within the same terms the qualifications and competences of the auditors in order to be able to assess any conflicts of interest;

b) forward to the Controller, without undue delay, any request from the Data Subjects that may be received by the Controller;

c) process information that does not consist of the customer's personal data, even after termination, for the purpose of feeding protection heuristics related to the Services;

d) recourse, against the Data Controller, of the part of the sum, if any, paid by way of compensation for the damage suffered by the Data Subject, corresponding to the Data Controller's share of liability.

**7. Obligations of the data Processor**

7.1. The Processor is obliged to:

a) performing the processing in accordance with the DPA and following any further lawful written instructions given by the Controller, if and to the extent that they comply with the privacy legislation and applicable regulations;

b) where applicable, provide due cooperation to the Data Controller to enable it to provide Data Subjects with information on the Processing of Personal Data in accordance with Articles 13 and 14 of the GDPR, as well as the collection of consent and its possible documentation (by means of keeping documents paper, log files, other computer documents);

c) put in place in advance, taking into account the state of the art and the costs of implementation, all the technical and organisational measures that are most appropriate and, in any case, adequate to the processing to ensure its security, considering the Processing itself in all its aspects, and considering in particular the risk on the rights and freedoms of the Data Subjects, and with specific reference to the provisions of Article 32 of the GDPR;

d) list the security measures taken in Appendix B;

e) indicate the other Data Controllers in Appendix C, and bind them to obligations ensuring at least the same level of Data protection as provided for in the DPA;

f) provide the Authorised Persons and/or System Administrators with instructions concerning the need to respect confidentiality and the prohibition of disclosure and/or dissemination of data, as well as to issue them with written instructions complying with the Regulations and to supervise their actions;

g) inform the Controller without undue delay of possible breaches of personal data of which it becomes or may become aware concerning its systems directly instrumental to the provision of the Services;

h) delete the Personal Data (and any existing copies) within a period of 60 days after Termination of the Agreement ("Main Agreement"), without prejudice to the right set out in Article 8.2.f below in relation to information that is not Personal Data;

i) provide the Controller with the widest possible cooperation in order to comply with the obligations imposed on the latter by the Applicable Legislation strictly related to the performance of the Contract and the RedHab Platform Licence Terms and Conditions, such as (by way of example only) those relating to security, to keeping a record of processing activities, to carrying out an impact assessment, to notifying a data breach, to communicating the breach to the Data Subjects;

j) cooperate with the Controller in the implementation of any requirements that may be imposed by a Regulatory Authority in any way or to any extent relevant to the performance of the RedHab Platform Licence Conditions and the DPA;

k) provide the fullest cooperation to the Data Controller for the purpose of responding to requests from Data Subjects involving the acquisition of information held by the Data Controller.

**8. Rights of the Parties**

8.1. The Controller is entitled to:

a) inform the Processor about which of the information, among those listed in Appendix A for each Service, it does not wish to collect; to this end, it undertakes to send a written communication to RedAbissi;

b) requesting the cooperation of the data processor, where possible and taking into account the nature of the processing, in activities relating to the data controller's obligation to comply with requests for the exercise of rights made by data subjects in accordance with the privacy legislation;

c) make use of other Data Processors in relation to the Data and/or Processing activities on the Data similar to those required for the purpose of the execution of the RedHab Platform Licence Terms and Conditions.

8.2. The Processor is empowered to:

a) make use of other third parties in the performance of the processing; to this end, the processor undertakes to inform the customer of any changes concerning the addition or replacement of the subjects to whom he entrusts the performance of the processing, thus giving the customer the opportunity to object to such changes, which shall be deemed approved in the absence of explicit objection within 7 (seven) days of the communication;

b) reserve the right to charge the Controller for the costs and expenses incurred in connection with audits, review and/or inspection activities, if they arise from the Controller's verified failure to comply with the obligations set out in the applicable Legislation or failure to comply with the RedHab Platform Licence Conditions or the DPA;

c) transfer (by means of communication, transmission and/or making available) the personal data, directly and/or by means of another Data Controller (indicated in Appendix C or subsequently identified and approved by the Data Controller), also outside the European Economic Area or to an international organisation, guaranteeing in all cases compliance with the guarantees or exceptions provided for in Chapter V of the GDPR;

d) inform the data controller if the law of the state of its nationality provides for an obligation to transfer the data outside the European Economic Area, unless such information is prohibited by law for important reasons of public interest;

e) inform the Controller in the event that an instruction given by the latter does not, in its opinion, comply with the privacy legislation and/or the instructions set out in the DPA;

f) give notice to the Controller of the deletion of any Databases, upon Termination, without prejudice to the right to retain, for the purposes of feeding the protection heuristics related to the Services, information from which it is unable to re-identify Users.

**9. Contacts of RedAbissi**

9.1 Contacting RedAbissi. The Data Controller has the right to contact RedAbissi, in relation to everything contained in this Data Processing Agreement, by writing an e-mail to help@redabissi.com or by pec: redabissi@pec.it .

**10. Conflicts**

10.1 Conflicts between the Parties' Agreements. In the event of any conflict or inconsistency between the provisions of the Agreement, the Processing Agreement and the Additional Instructions, unless otherwise provided in this Processing Agreement, the following order of precedence shall apply: (a) the Additional Instructions; (b) the remaining provisions of the Processing Agreement; and (c) the remaining provisions of the Agreement. Subject to any amendments to the Processing Agreement, the Agreement shall remain in full force and effect.

10.2 Violations of laws or regulations. Any provision of the Agreement, the Processing Agreement and/or the Additional Instructions that is contrary to European or national law shall be deemed to be unreported and fully replaced by the violated provision if it cannot be derogated from by agreement between the parties

**11. Express acceptance.**

11.1 Pursuant to and for the purposes of the applicable legislation, the User further declares that he/she has read and expressly accepted without reservation the following clauses: 2, 3, 4, 5, 6, 7, 8, 9, 10 and also Appendix 1 (Object of data processing), Appendix 2 (Technical and organisational security measures) and Appendix 3 (Sub-processors).

**APPENDIX 1: PURPOSE AND DETAILS OF DATA PROCESSING**

**Object**
The provision of an online digital platform that allows the user to directly and in-house manage marketing campaigns and online communications, through the use of different messaging channels and as further defined in the Customer Agreement ("Main Agreement") and the RedHab Platform Licence Terms and Conditions.

**Duration of treatment**
For the contractual period of validity plus an additional period of 60 (sixty) days from the termination of the contract - in accordance with the Data Processing Agreement signed with the Customer ("Main Agreement").

**Nature and purpose of the processing of the Processor's Services**
RedAbissi shall process the Customer's Personal Data in order to provide the contracted services in accordance with the instructions contained in this Data Processing Agreement.

Depending on the Processor's Services chosen in the Contract, the Customer's Personal Data may include the following:

- Common identification data (e.g. first name, surname, address, e-mail, telephone number);
- Data relating to sole proprietorships or one-man companies in combination with possible common contact data (telephone or e-mail) provided by the Customer relating to persons directly or indirectly involved in the "Main Agreement" with the Customer;
- User data collected by tracking technologies and devices where not disabled by the Client;
- Any further personal data of common origin entered by the Customer or User on the RedHab platform (which cannot be determined beforehand).

**Types of stakeholders involved**

- Customer Contacts
- sole proprietorships or unipersonal companies of persons involved directly or indirectly in the "Main Agreement" with the Customer.
- Target audiences for social campaigns
- Common data or electronic identification data of recipients of communications sent by the Customer through the Services of the Processor through the use of the RedHab platform

The parties may update the list of types of personal data processed in the provision of the Processor's Services from time to time**.**

From time to time, RedAbissi may update or amend these Security Measures, provided that such updates and amendments do not result in a deterioration of the overall security of the Processor's Services or otherwise a decrease in the agreed level of security.

**APPENDIX 2: TECHNICAL AND ORGANISATIONAL SECURITY MEASURES**

The Data Processor adopts the following technical and organisational security measures pursuant to Article 32 of the GDPR. The Data Processor works constantly to improve its security measures and to keep them up-to-date with technological developments.

**A. TECHNICAL MEASURES**

A-1) Authentication Credentials - Access to the systems is based exclusively on unique authentication credentials, based on a confidential PIN or access key and with security measures that comply with international standards;

A-2) Management of access passwords according to best practices, based on length, complexity, expiry, robustness entrusted to persons duly trained in its use and storage;

A-3) System Administrators - For users with the role of System Administrators, whose duties are assigned by specific written appointment acts, a duly configured, non-alterable log management system is implemented to track the activities performed and allow subsequent monitoring to verify the regularity of operations;

A-4) Use of encryption systems based on computer algorithms and protocols conforming to international standards;

A-5) IDS/IPS Intrusion Detection System and Intrusion Prevention System as intrusion detection systems to detect cyber-attacks in advance;

A-6) Adoption of firewall systems as perimeter defence components of computer networks and to protect communication lines;

A-7) Logging systems for the purpose of monitoring systems, storing events and identifying accesses;

A-8) Backup & restore systems and their management procedure;

A-9) Business continuity for system resilience in the event of an incident;

A-10) Vulnerability Assessment & Penetration Tests - System vulnerability analyses are carried out periodically in relation to both infrastructural and application areas, and Penetration Tests are performed periodically, assuming different attack scenarios, with the aim of verifying the security level of applications/systems/networks and then, on the basis of the relevant reports, improving security measures;

A-11) Choice of Data Centres with Tier 3 or higher standards in ISO 9001 and ISO 27001 certified facilities;

A-12) Constant updating of IT systems, technical measures, as technology changes and with constant verification according to pre-established timetables, as well as constant verification, from reliable sources, of the security problems of IT products and services in use for the relevant update

**B. ORGANISATIONAL MEASURES**

B-1) Adoption of an information security management policy and a personal data protection policy in accordance with privacy legislation, based on risk analysis, to ensure the confidentiality, availability and integrity of personal data to protect the rights and freedoms of data subjects;

B-2) Procedures for access to physical facilities, duly secured, only to authorised persons after appropriate authentication;

B-3) User Policies and Disciplinary: Detailed policies and disciplines are applied, with which all users with access to IT services must comply to guarantee the security of the systems;

B-4) Logical access authorisation - All computer systems are accessible only with access profiles as required for the task being performed. Authorisation profiles are identified and configured prior to access;

B-5) Existence of an incident management procedure linked to technical tools for monitoring the systems assigned to specialised personnel, with the identification, in the event of an incident, of the actions to be taken in a logically

determined order, with the aim of ensuring the restoration of the services in the shortest possible time, as well as verifying the consequences, drafting a report, on the outcome of which further protection measures depend, without prejudice to the verification of the adequacy of the protection systems in place;

B-6) Support management procedure - Support interventions are managed by means of a procedure that verifies the authenticity of the request and provides support while keeping the processing of personal data to a minimum, by means of duly trained personnel and technical tools that comply with security standards. Also, by means of a ticket system service made available to the CUSTOMER, it will always be possible to know the details of the intervention, duration, date and the operator (by means of a unique code assigned to him/her), as well as to verify the authenticity of the support request;

B-7) Levels of access to systems and defined 'permissions' to provide technical assistance, assigned only to certain specifically authorised employees with authentication credentials conforming to international standards;

B-8) Commitment to confidentiality in writing by all employees before accessing the systems;

B-9) Defined corporate privacy organisation chart: each employee may only process information for which he or she has been authorised in relation to the duties performed and duly trained, through periodic updates, to process data with the utmost confidentiality and security, in compliance with privacy regulations;

B-10) Internal rules for employees on the use of IT tools and potential employer controls;

B-11) Procedures to protect against social engineering attacks with associated specific staff training;

B-12) Procedures for the selection of suitable suppliers focused on verifying the quality, safety and regulatory compliance of the goods or services offered;

B-13) Data Breach - Internal procedures for incident management, based on the distribution of roles according to competence, management of countermeasures, as well as the modalities for sharing information on personal data breaches with the customer and for the adoption of related obligations under privacy regulations;

B-14) Procedures for the disposal of analogue documentation and computer systems potentially containing information, using appropriate means (such as document shredders and certified disposal companies);

B-15) Physical measures for the protection of working and storage environments (anti-theft systems, fire-fighting systems, etc.);

B-16) Update of organisational measures to be reviewed every six months;

**APPENDIX3: SUB-PROCESSORS**

| Name | Head Office | Place of processing | Areas of processing |
|---|---|---|---|
| Neten srl | Via Gianfranco Zuretti 34, 20125 Milano Mi | Italy, European Union | Cloud Computing Provider for RedAbissi S.r.l. |
| Irideos spa | Viale Bodio 37, 20158 Milano | Italia, Unione Europea | Cloud Computing Provider per Redabissi Srl |
| . | | | |
| | | | |
| | | | |
| | | | |