Why a Processor Annex?

As from May 25th 2018 onwards the European General Data Protection Regulation ("GDPR") became effective. We highly value a careful handling of personal data and expect this from organizations we work with as well.

When using our services on your end, and when performing our services on our end, both of us will share data with the other party. Data that you, as a brand (representative), will gain access to are: the company name of our users, the geolocation of our users and data about their usages of our app. Data that we will gain access to from you are: (Company) name of your clients and their email address.

From a legal point of view, we cannot guarantee that all company names and email addresses are not personal data. That is why we enter into a Data Processing Annex with you in which the above-mentioned exchange of data is stated. This document describes that and how our organizations process personal data and that they only use the (personal) data in line with the purpose of this agreement.

Data Controller versus Processor

When using our Software and App, we grant you access to our platform where personal data might be processed. Since we, on this platform, determine means and goals of this personal data processing, we see ourselves as responsible for the personal data in our platform, in other words, as Controller of the personal data. When, in turn, we give your organization access to the platform, your organization may access and use certain personal data for its own purposes. In this context, each party acts as an independent controller for its own processing activities and is responsible for complying with its respective obligations under the GDPR.

When you are using our campaign services, you determine purpose and means of the processing of any personal data. In that regard, you control the personal data that you may share with us. We only use such data on your instructions. Therefore, when using our campaign services, you qualify as a Controller of the personal data whereas we are the Processor.

Data Processing Annex

Parties

1. The private company with limited liability Embrosa B.V., with registered office at (5928 NL) Venlo at Kazernestraat 17, legally represented by Melanie van Norden, hereinafter referred to as: "Embrosa"

and

2. The Customer, hereinafter referred to as: "Customer"

Jointly hereinafter also referred to as "Parties", Consider the following

A. Depending on the exact nature of their collaboration, both Parties may be considered data controller ("Data Controller") and/or data processor ("Data Processor"). The terms Data Controller and Data Processor shall have the meaning as defined in article 4.7 respectively 4.8 of the GDPR. When referring to Data Controller or Data Processor in this Annex, the party fulfilling that particular role in the sense of the GDPR is meant;

B. The Processor obtains access to (personal) data pertaining to the responsibility of the Controller, through or via the IT platform of the Controller, or in any other way, and processes personal data for the Data Controller within this context;

C. The Data Controller carries responsibility for the processing of personal data and is recognized as the Data Controller within the meaning of Article 4 of the GDPR;

D. The Data Processor, in respect of the storage and processing of the personal data, is recognized as the Data Processor within the meaning of Article 4 of the GDPR;

E. The Parties also wish – with regard to the provisions of Article 28, third paragraph of the GDPR - to establish in this annex specific conditions that apply to their relationship in connection with the processing of personal data for the Data Controller.

And agree to the following:

Article 1. Definitions

1. The following capitalized terms have the following meanings:

AP:	the Dutch supervisory authority Autoriteit Persoonsgegevens;
Customer:	the party using the Embrosa platform and/or campaign services to; a). to provide its (potential) customers (retailers and resellers) with access to the (Marketing) content added by Customer, b). to distribute the added (Marketing) content among her (potential)customers and/or c). to gain insights in the use of (Marketing) content by its (potential) customers. (*In human speak 'the Brand'.)*
Users:	the end users of Embrosa's platform services who receive (Marketing) information and participate in campaigns from Controller and Processor; *(In human speak 'the Retailers and Resellers.)*
End Consumers	the final consumer buying the products or services your company offers; *(in human speak ' the End Consumer')*
GDPR:	the General Data Protection Regulation;
Personal Data Breach:	a breach of the security of Personal Data that inadvertently or unlawfully leads to the destruction, loss, modification or unauthorized disclosure of or unauthorized access to transmitted, stored or otherwise processed data;
Agreement:	the (commercial) agreement concluded between the Data Controller and the Data Processor, under which the Data Processor shall Process Data Controller Personal Data;

Personal Data:	all data that can be traced directly or indirectly to a natural person as referred to in Article 4 of the GDPR;
Processing:	the processing of Personal Data as referred to in Article 4 of the 2 GDPR;
Data Processing Agreement:	the present agreement which forms part of the Agreement;

2. The provisions of the Agreement shall apply in full to the Data Processing Agreement. With regard to the processing of Personal Data, the provisions of this Data Processing Agreement always apply.

Article 2. Data Controller and Data Processor of Personal Data

1. The Data Processor shall process Personal Data on behalf of the Data Controller in the execution of the Agreement. The provisions of this Data Processing Agreement shall apply to this Processing.

2. The Processing relates to the following categories of persons involved:
   - Users of the service of the Data Controller
   - End Consumers of the service of the Data Controller

3. The processing shall take place for the following purposes and concerns the following categories of Personal Data:

Service

Purpose:	Providing the service Handling complaints Commercial activities including sales and advertisements
Categories of Personal Data:	(Company) name of the User, (Company) email address, User number *(an identifier in the Embrosa platform or the systems of Customer)*, Company address, (Company) phone-number, Click behavior, Surf behavior, Personal Photo and any further information provided by the User or Customer or End Consumer

Marketing

Purpose:	General marketing activities including,but not limited to: ● Direct marketing ● Newsletter ● Social media marketing ● Advertising ● Behavioral targeting ● Loyalty program

Categories of Personal Data:	Click behavior, Surf behavior, Username, Company name, Company Location, (Company) name, and any further information provided by the User or Customer or End Consumer

Product sales

Purpose:	Handling complaints chat contact, sales, and advertisement
Categories of Personal Data:	(Company) name of the User, (Company) email address, User number *(an identifier in the Embrosa platform or the systems of Customer)*, Company address, (Company) phone-number, Click behavior, Surf behavior and any further information provided by the User or Customer or End Consumer

4. The Data Processor shall only process the Personal Data for the activities mentioned in this Data Processing Agreement and the Agreement. The Processor shall not make use of the Personal Data in any other way unless the Controller has given explicit and written permission otherwise, or a statutory provision obliges the Processor to do so. In that case, the Processor shall inform the Controller, before the Processing takes place, of the statutory provision, unless such a process is not permitted by this legislation.

Article 3. General duty of care Data Processor

1. The Processor must ensure compliance with this Data Processing Annex and the statutory rules (such as the GDPR) that apply to the Processor. If the Controller so requests, the Processor shall inform the Controller of the actions and measures taken by the Processor within the framework of this general duty of care.

Article 4. Technical and organizational measures

1. The Processor shall take appropriate technical and organizational measures to secure the Personal Data against loss or unlawful Processing. The Processor must ensure that the security level sufficiently addresses the risks. These measures will take into account the current state of technology and the costs of the security measures.

2. The Processor shall, in any case, take measures to protect the Personal Data against destruction, against accidental and intentional loss, forgery, unauthorized distribution or access, or against any other form of unlawful Processing.

3. The Processor shall assist the Controller in fulfilling the security obligations that rest on the Controller himself.

4. The Processor shall, at first request of the Controller, provide a document which includes the technical and organizational measures taken by the Processor.

Article 5. Confidentiality

1. The Processor shall have all employees who are involved in the execution of the Agreement sign a confidentiality agreement - whether or not resulting from or included in the employment contract with those employees - which states that these employees must observe confidentiality with regard to the Processing of the Personal Data. The Processor shall take all necessary measures, such as screening of employees and security of data carriers, to ensure that confidentiality is maintained.

Article 6. Data processing outside the European Economic Area (EEA)

1. Processing of Personal Data outside the EEA shall only take place if and insofar as one of the following two conditions is met:

(i) a formal adoption on appropriate level of protection of the European Commission under the applicable data protection legislation shall apply to that country or territory; or

(ii) The party processing outside the EEA complies in full with the requirements of the European Commission Decision of 4 June 2021 on Standard Contractual Clauses (Module two, transfer Controller to Processor) for the transfer of personal data to third parties pursuant to the GDPR, attached as Appendix A, or any other clauses or requirement as adopted by the European Commission from time to time.

Article 7. Sub-processors

1. The Processor is allowed to make use of sub-processors in the framework of the Data Processing Annex and the Agreement.

2. The processor obligates each sub-processor to fulfill the confidentiality obligations, notification obligations, and security measures in relation to the Processing of Personal Data, which obligations and measures must at least comply with the provisions of this Data Processor Annex.

Article 8. Liability

1. The Processor is liable to the Controller for all damage and costs in connection with a claim from a data subject, which is the result of the fact that the Processor has failed to comply with the obligations arising from the GDPR or has acted contrary to the lawful instructions of the Controller.

Article 9. Infringement in connection with Personal Data (Data Breach)

1. If the Processor is informed of a Data Breach, the Processor shall (i) inform the Controller as soon as possible and in any case within 24 hours after the Processor became aware of the existence of the Data Breach and (ii) take all reasonable measures to limit or prevent (further) violation of the GDPR. When taking the aforementioned measures, the Processor shall refrain from taking measures that are irreversible and/or seriously impede an investigation into the causes of the Data Breach.

2. The Processor shall offer cooperation and support to the Controller in the performance of its legal obligations with respect to the identified incident.

3. The Processor shall offer technical support to the Controller with regards to the reporting obligation with respect to the Personal Data Breach with the Dutch Data Protection Authority ("Autoriteit Persoonsgegevens" or "AP") and/or the person concerned, as referred to in Article 33 paragraph 3 and 34 paragraph 1 GDPR. The Processor shall refrain from independently submitting a notification of infringement related to Personal Data to the AP and/or the Data Subject.

Article 10. Assistance to Data Controller

1. Under the GDPR, the Data Subject has a number of rights, including the right of access (Article 15 of the GDPR), rectification (Article 16 of the GDPR), right to erasure (Article 17 of the GDPR), right to restrict the processing of personal data (Article 18 of the GDPR), data portability (Art. 20 GDPR) and the right of objection (Articles 21 and 22 GDPR). The Controller must answer requests for the exercise of those rights and the Processor will provide support to the Controller in so far as reasonably possible. For example, if the complaint is submitted to the Processor, the Processor will forward the complaint or request from a Data Subject to the Controller as quickly as possible.

2. The Processor shall support the Controller, as far as reasonably possible, in fulfilling its duty under the GDPR to carry out a Data Protection Impact Assessment (articles 35 and 36 GDPR).

3. The Processor shall provide the Controller with all information necessary to demonstrate that the Processor complies with its obligations under the GDPR. In addition, at the request of the Controller, the Processor will make and contribute to audits, including inspections, by the Controller or a party authorized by the Controller.

Article 11. Termination & Miscellaneous

1. With regard to the termination of this Data Processing Annex, the specific provisions of the Agreement apply. Without prejudice to the specific provisions of the Agreement, the Processor will delete or return all Personal Data at the first request of the Controller, and delete existing copies, unless the Processor is otherwise legally obliged to store the Personal Data.

2. The retention period of the Personal Data is normally 36 months after the last documented interaction that is directly related to the purpose for which the Personal Data are processed, unless the Processor is otherwise legally obliged to keep the Personal Data on for a longer or shorter period of time (in which case the maximum retention period will be equal to that legally imposed period). The Processor will no longer process the Personal Data or store it in accordance with this retention period. Personal Data obtained by the Processor without using the services of the Controller do not fall within the specified retention period.

3. In the event that the Controller discloses a request for erasure of Personal Data from a User or End Consumer to the Processor, the Processor will delete this Personal Data within a maximum period of one month after the notification.

4. The Processor will ensure adequate technical and organizational security measures are implemented.

5. The obligations arising from this Data Processing Annex which by their nature are intended to survive termination shall also remain in force after termination of this Data Processing Agreement.

6. This agreement is governed by Dutch law and is translated into the English language.

APPENDIX A - Standard contractual clauses

These are the Standard Contractual Clauses, as mentioned in Article 6 of the Data Processing Annex of Embrosa B.V. which apply to all who process data outside the European Economic Area (EEA).

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1. Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses")

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2. Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3. Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4. Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5. Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6. Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional. Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8. Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the

duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9. Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the

sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fullfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fullfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10. Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11. Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion.

The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12. Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13. Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14. Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

  (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

  (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

  (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fullfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract

involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15. Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required

to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16. Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

  (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

  (ii) the data importer is in substantial or persistent breach of these Clauses; or

  (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

  In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17. Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

Clause 18. Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Netherlands.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

Annex I

A. LIST OF PARTIES

Data Exporter *(Brand / Customer)*:

Name:

Address:

Contact person of Customer:

Name:

Position:

Contact details:

☐ Contact person is data protection officer ☐internal ☐external

Activities relevant to the data transferred under these Clauses:

Click or type here to enter the activities.

Role: When using campaign services: Customer = Controller ☐X Controller ☐Processor	Signature Customer Date Place
First and last name:	

Role: When access to the platform: Customer = independent Controller X Controller ☐ Processor	Signature Customer Date Place
First and last name:	

Data Importer:

Name: Embrosa B.V.

Address: De Manufactuur, Kazernestraat 17, 5928 NL Venlo, The Netherlands

Contact person of Embrosa B.V.:

Name: Melanie van Norden

Position: CEO

Contact details: melanie@embrosa.com | +31-85-3038686

X Contact person is data protection officer

X internal

X external

Activities relevant to the data transferred under these Clauses:

Role: When using campaign services: Embrosa = Processor ☐ Controller X Processor	Signature Embrosa Date Place
First and last name: Melanie van Norden	

Role: When access to the platform: Embrosa = independent Controller X Controller ☐ Processor	Signature Embrosa Date Place
First and last name: Melanie van Norden	

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

X Customers	☐ Event participants
☐ Relatives of employees	☐ Potential customers
☐ Visitors	☐ Applicants
☐ Employees	☐ Business partners
☐ Apprentices	☐ Suppliers
☐ Communication participants	☐ Trainees
☐ Students	☐ Authorized agents
☐ Shareholders	X Contact persons
☐ Suscribers	X End Consumer (Landingpage only)
☐ Other category	☐ Other category

Categories of personal data transferred

X Names	☐ Factors specific to the physical identiity
☐ Identification number	☐ Factors specific to the physiological identiity
X Location data	☐ Factors specific to the genetic identiity
☐ Online ident	☐ Factors specific to the mental identiity
	☐ Factors specific to the economic identiity
	☐ Factors specific to the cultural identiity
	☐ Factors specific to the social identiity

X Customer data	☐ Data of event participants
☐ Data of relatives of employees	☐ Data of potential customers
☐ Data of visitors	☐ Data of applicants
☐ Data of employees	☐ Data of business partners
☐ Data of apprentices	☐ Data of suppliers
☐ Data of communication participants	☐ Data of trainees
☐ Data of service providers	☐ Data of consultants
☐ Data of students	☐ Data of authorized agents
☐ Data of shareholders	X Data of contact persons

☐ Data of suscribers	☐ Other category

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

☐ Racial origin	☐ Ethnic origin
☐ political opinions	☐ Religious beliefs
☐ Philisophical beliefs	☐ Trade union membership
☐ Genetic data	☐ Biometric data
☐ Data concerning health	☐ Data concerning sex life
☐ Data concerning sexual orientation	☐ Data relating to criminal convictions
☐ Data relating to criminal offences	☐ Other category
☐ Other category	☐ Other category

The frequency of the transfer

☐ The data is transmitted once.

X The data is transmitted continuously.

☐ Click or type here to enter text.

Nature of the processing

☐ Collection	☐ Adaption	☐ Disclose by transmitting
☐ Restriction	☐ Recording	☐ Alteration
☐ Dissemination	☐ Erasure	☐ Organisation
☐ Retrieval	X Making available	☐ Destruction
X Structuring	☐ Consultation	☐ Alignment
☐ Storage	X Use	☐ Combination
☐ Click or type here to enter text.		

Purpose(s) of the data transfer and further processing

The controler is sharing a list of customers that want to participate in the Hyper-local (advertising) Campaign. The controler informs these customers that Embrosa will contact them. Embrosa then contacts the Customers/Companies:

a. asking them to give legal permission to Embrosa to publish one specific campaign on the social media channels of their Company;
b. asking them give technical permission to Embrosa to publish on the social media channels of their Company; (a.k.a.Connect the Companies' social media accounts;

c. inform them about the start, finish, progress and results of the campaign.

Embrosa uses the data to contact the Companies and set up the advertising campaign for their specific Company.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

☐ The data is stored for a short time: Click or type here to enter text.

☐ The data is stored for a long time: Click or type here to enter text.

☐ The duration of the storage results from the main contract.

X The duration of the storage results from the legal storage periods.

X The participants' list is stored in accordance with the retention period as set out in Article 11.2.

X Customer communication is stored in our CRM system until the customer requests the removal of the data.

For transfers to (sub-) processors, also specify the subject matter, nature, and duration of the processing.

(Sub) Processor Number	Subject Matter	Nature	Duration of Processing
Embrosa	Customer Data - (Company) Name - Company Address - (Company) Email address - (Company) phone number - (Company) photo/video - Facebook Page ID - Instagram Page ID	- Structuring (overview (status) Participants) - Use (to set up Ads) - Use (to check overlapping radii of Companies/Participants based on Copmany Address) - Use (to communicate with participants about) the campaign) - Use to personalize ads with (Company) photo/video	- Start: when participants list is shared by Controller - Finish: in accordance with the retention period as set out in Article 11.2. - Finish in SP0002: upon request by data subject
SP0001 Google Cloud, & Google Workspace,	Customer Data - (Company) Name - Company Address - (Company) Email address - (Company) phone number - (Company) photo/video - Facebook Page ID - Instagram Page ID	- Structuring (overview (status) Participants) - Use (to set up Ads) - Use (to check overlapping radii of Companies/Participants based on Company Address) - Use to personalize ads with (Company) photo/video	- Start: when participants list is shared by Controller - Finish: in accordance with the retention period as set out in Article 11.2.
SP0002	- deleted in 04/2026	-	-

Freshworks (CRM)			
SP0003 (Media Meisters)	- deleted in 04/2026	-	-
SP0004 (Multiply)	- deleted in 04/2026	-	-
SP0005 (META)	Customer Data - (Company) Name - Company Address - (Company) photo/video - Facebook Page ID - Instagram Page ID - (Company) Phone Number	- Make available (Company name is entered as name for the Adset) - Make available (Company address is entered as location for hyper-local targeting) - Use (to set up Ads) - Use to personalize ads with (Company) photo/video - WhatsApp Used (to answer questions from Customers/Users/Companies and to deliver advise/tips)	- Start: 2 weeks before start campaign - Finish: in accordance with the retention period as set out in Article 11.2. *Be aware: All data (Company) Name, Company Address, Facebook Page ID and Instagram Page ID) were already known to META before Embrosa had set up a campaign. So although Embrosa stops sharing the data with META, the data is still stored in META's databases.*
SP0006 Gleap GmbH (CRM)	Customer Data - (Company) Name - Company Address - (Company) Email address	- Use (to communicate with participants about the campaign) - Use (to answer questions from Customers/Users/Companies)	- Start: when participants list is shared by Controller - Finish: in accordance with the retention period as set out in Article 11.2.
	- Mobile Phone Number	- Use (to answer questions from Customers/Users/Companies)	- Start: when participant asks Embrosa a question through WhatsApp - Finish: in accordance with the retention

			period as set out in Article 11.2.
SP0007 Google Ads	Customer Data - (Company) Name - Company Address - (Company) photo/video	- Make available (Company name is entered as name for the Campaign) - Make available (Company address is entered as location for hyper-local targeting) - Use (to set up Ads) - Use to personalize ads with (Company) photo/video	- Start: 2 weeks before start campaign - Finish: in accordance with the retention period as set out in Article 11.2.
SP0008 Vistar Media (Digital Out Of Home Ads)	Customer Data - (Company) Name - Company Address - (Company) photo/video	- Make available (Company name is entered as name for the Digital Out Of Home Campaign) - Make available (Company address is entered as location for hyper-local targeting) - Use (to set up Ads) - Use to personalize ads with (Company) photo/video	- Start: 2 weeks before start campaign - Finish: in accordance with the retention period as set out in Article 11.2.
SP0009 Voys	Customer Data - (Company) Name - Phone Number	- Use (to answer or call (back) customers - Use (to answer questions from Customers/Users/Companies)	- Start: when a Customer calls Embrosa's phone number - Finish: in accordance with the retention period as set out in Article 11.2.

Signature Customer	Signature Embrosa Melanie van Norden
Date	Date
Place	Place

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13.

Autoriteit Persoonsgegevens (Dutch Data Protection Authority)

Annex II

Technical and organizational measures including technical and organizational measures to ensure the security of the data in accordance with Art. 32 GDPR

Date:

Organisations that collect, process, or use personal data themselves or on behalf of others must implement the technical and organizational measures necessary to ensure they comply with data protection laws. Measures are only deemed necessary if the effort required to implement them is proportionate to the intended protective purpose.

The abovementioned organization fulfills these requirements with the following measures:

1. Confidentiality pursuant to Art. 32(1) GDPR

1.1. Access (entry) control

Measures appropriate to deny unauthorized persons access to data processing facilities with which personal data are processed or used. Access control measures securing buildings and spaces may include automatic access control systems, the use of smartcards and transponders, the use of porter services, and alarm systems. Servers, telecommunications facilities, network technology, and similar facilities should be protected in lockable server cabinets. It is also sensible to support access control with organizational measures (e.g. instructions requiring rooms to be locked when not occupied).

**** Additional information: Embrosa works remote-first. Most Embrosians work most of the time from home. We hire a flex office, that offers alarm systems with various security features, but during workdays, other organizations which hire a flex office and their guests can access this office freely too. We however do not store any personal data in print. We focus heavily on protecting the digital office a.k.a. the safety of the laptop/computer of the Embrosians.*

Technical measures	**Organisational measures**
X Alarm system **** available in flex office*	☐ Key regulations/list
☐ Automatic access control systems	☐ Reception/porter services
☐ Biometric entry barrier	☐ Visitor book/record of visitors
X Smartcards / transponder systems **** available in flex office*	☐ Staff/visitor passes
X Manual locking system **** available in home office*	☐ Visitors accompanied by staff

X Security locks **** available in flex office*	☐ Due care when selecting security personnel
☐ Locking systems with code locks	☐ Due care when selecting cleaning services
☐ Protection of building shafts	☐ Other measure
☐ Doors with handles on the outside	☐ Other measure
☐ Doorbells with camera facilities	☐ Other measure
X Video surveillance of entrances	☐ Other measure
☐ Other measure	☐ Other measure
☐ Other measure	☐ Other measure
☐ Other measure	☐ Other measure

1.2. System access control

Measures appropriate to prevent unauthorised persons using data processing systems (computers). System access control means preventing the unauthorised use of facilities. Possible controls include boot passwords, user recognition passwords for operating systems and software products, screensavers with passwords, smartcards for registration and the use of call back procedures. Organisational measures may also be necessary, for example to prevent unauthorised inspection (e.g. guidelines for screen set up, issuing guidance to users on selecting "good" passwords).

Technical measures	**Organisational measures**
X Login with username + password	X User authorisation management
☐ Login with biometric data	X Setting up user profiles
☐ Anti-virus software for servers	X Central password allocation
☐ Anti-virus software for clients	X "Secure password" guideline
☐ Anti-virus software for mobile devices	X "Deletion/destruction" guideline
☐ Firewall	X "Clean desk" guideline
☐ Intrusion detection systems	X General data protection and/or security guideline
☐ Mobile device management	☐ Mobile device policy
X Using personal VPN for remote access	X "Manual desktop lock" instructions
☐ Encryption of data carrier	X Signed NDA by employees
☐ Encryption of smartphones	☐ Other measure

☐ Case lock	☐ Other measure
☐ BIOS protection (separate password)	☐ Other measure
☐ Blocking external interfaces (USB)	☐ Other measure
☐ Automatic desktop lock	☐ Other measure
X Encryption of notebooks/tablets	☐ Other measure
X 2FA if available	☐ Other measure
X Google Cloud Platform Security Compliance	☐ Other measure

1.3. User access control

Measures guaranteeing that the persons authorised to use a data processing system can only access the data they are authorised to access and that personal data cannot be read, copied, altered or removed without authorisation, while being processed or used or following storage. User access control can also be guaranteed by appropriate authorisation concepts that enable data access to be controlled in a differentiated manner. This means that the data content, as well as possible data access functions, must be differentiated. Appropriate control mechanisms and responsibilities must also be defined so that the granting and removal of authorisations is documented and kept up to date (e.g. upon employment, change of workplace, termination of employment relationship). Particular attention must always be paid to the administrator's role and options.

Additional information: Embrosa has no own servers. We make use of the Google Cloud Platform. Google has included many safety features in their servers and services https://cloud.google.com/security.

Technical measures	**Organisational measures**
☐ File shredders (minimum level 3, cross cut)	X Use of authorisation concepts
☐ External file shredder (DIN 66399)	☐ Minimum number of administrators
☐ Physical deletion of data carrier	☐ Data protection safe
☐ Recording access to applications, specifically when inputting, altering and deleting data	X User rights management by administrators
☐ Other measure	☐ Other measure
☐ Other measure	☐ Other measure

1.4. Separation control

Measures guaranteeing that data collected for different purposes can be processed separately. This can, for example, be guaranteed by the logical and physical separation of data.

Technical measures	Organisational measures
☐ Separation of productive and test environments	☐ Control of authorisation concept
X Physical separation (systems/databases/data carrier)	☐ Determination of database rights
☐ Multi-client capability for relevant applications	☐ Datasets assigned purpose attributes
☐ Other measure	☐ Other measure
☐ Other measure	☐ Other measure

1.5. Pseudonymisation (Art. 32(1)(a) GDPR; Art. 25(1) GDPR)

Processing personal data in such way that the data can no longer be assigned to a specific person without reference to additional information, provided that this additional information is kept separately and is subject to appropriate technical and organisational measures.

Technical measures	**Organisational measures**
☐ Where pseudonymisation is used: separation of assignment data and storage in separate and secure systems (possibly encrypted)	X Internal instruction to anonymise / pseudonymise personal data in the event that it is transferred or after the expiry of the statutory erasure deadline
☐ Other measure	☐ Other measure
☐ Other measure	☐ Other measure

2. Integrity (Art. 32(1)(b) GDPR)

2.1. Transfer control

Measures guaranteeing that personal data cannot be read, copied, altered or removed without authorisation when being transferred electronically or transported or saved onto data carrier and that it is possible to verify and establish to which bodies the transfer of personal data by means of data transmission facilities is provided for. To guarantee confidentiality when data is transferred electronically, encryption technologies and virtual private networks may, for example, be used. Measures to be implemented when transporting or transferring data are transportation boxes with locking devices and rules for the destruction of data carrier in compliance with data protection laws.

Technical measures	**Organisational measures**
X Email encryption *Only for emails containing (files with) personal data.*	☐ Documentation of data recipients, as well as the duration of the planned transfer or erasure deadlines
☐ Using VPN	☐ Overview of regular retrieval and transmission processes
☐ Recording access and retrieval *only limited available in Gleap*	☐ Transfer in anonymised or pseudonymised form
☐ Secure transportation boxes	☐ Due care when selecting transport personnel and vehicles
X Provision via encrypted connections such as sftp, https	☐ Personal delivery with log
☐ Using signature procedures	☐ Other measure
☐ Other measure	☐ Other measure
☐ Other measure	☐ Other measure

2.2. Input control

Measures guaranteeing that it is subsequently possible to verify and establish whether and by whom personal data has been entered, altered or removed in data processing systems. Input control is achieved by logging on different levels (e.g. operating system, network, firewall, database, application). It must be clarified which data is logged, who has access to logs, by whom and on what occasion/time they are checked, how long storage is necessary and when the logs are deleted.

Technical measures	Organisational measures
X Technical recording of inputting, alteration and deletion of data *(Audit Log)*	☐ Overview of which programs can be used to input, alter or delete which data
☐ Manual or automatic monitoring of records	X Transparency of inputting, alteration and deletion of data by individual username (not user groups)
☐ Other measure	☐ Allocation of rights to input, alter and delete data based on a concept of authorisation
☐ Other measure	☐ Safekeeping of forms from which data are copied for automated processing
☐ Other measure	☐ Clearly defined responsibilities in respect of deletions

3. Availability and resilience (Art. 32(1)(b) GDPR)

3.1. Availability control

Measures guaranteeing that personal data is protected against accidental destruction or loss. This includes topics such as uninterruptible power supply, air conditioning systems, fire safety, data backups, secure data carrier storage, virus protection, raid systems, disk mirroring, etc.

Additional information: Embrosa has no own servers. We make use of the Google Cloud Platform. Google has included many safety features in their servers and services https://cloud.google.com/security, including X Backup & recovery, Monitoring security procedures, regular data recovery tests and result logging

Technical measures	Organisational measures
☐ Fire and smoke alarm systems	X Backup & recovery concept (formulated) *Through Google Cloud Platform*
☐ Fire extinguishers in server room	X Monitoring security procedures *Through Google Cloud Platform*

☐ Monitoring temperature and humidity in server room	☐ Regular data recovery tests and result logging
☐ Air conditioned server room	☐ Storing backup media in a secure location outside of the server room
☐ UPS	☐ No sanitary connections in or above the server room
☐ Safety power outlet strips in the server room	☐ Emergency plan (e.g. BSI IT-Grundschutz 100-4)
☐ Data protection safe (S60DIS, S120DIS, other appropriate norms with intumescent seal etc.)	☐ Separate partitions for operating systems and data
☐ RAID system/hard disk mirroring	☐ Other measure
☐ Video surveillance in server room	☐ Other measure
☐ Alarm signal on unauthorised access to the server room	☐ Other measure
☐ Other measure	☐ Other measure
☐ Other measure	☐ Other measure
☐ Other measure	☐ Other measure

4. Procedures for regular inspection, assessment and evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

4.1. Data protection management

Technical measures	Organisational measures
☐ Using software solutions for data protection management	X Internal/external data protection officer Name/company/contact details Melanie van Norden (Internal) | Embrosa B.V. | melanie@embrosa.com | 06-20908995
X Central documentation of all procedures and rules regarding data protection that is accessible to staff according to read/authorisation (our Embrosa: knowledge base SLAB)	☐ Staff are trained and have given undertakings in relation to confidentiality/compliance with the requirements of GDPR (data confidentiality)
☐ Security certification pursuant to ISO 27001, BSI IT-Grundschutz or ISIS12	X Staff awareness raised regularly, at least annually
☐ Other documented security concept Other document	☐ Internal/external information security officer Name/company/contact details Type here the name of security officer and contact details
☐ A review of the effectiveness of the technical protective measures takes place at least annually	☐ The data protection impact analysis is carried out as necessary
☐ Other measure	X The organisation complies with the information obligations contained in Articles 13 and 14 GDPR
☐ Other measure	X There is a formalised process for processing information requests from data subjects
☐ Other measure	☐ Other measure

4.2. Incident response management

Support in responding to security breaches

Technical measures	Organisational measures
☐ Using a firewall and regular updating *Not necessary with Google Cloud Platform*	X Documented process for the recognition and reporting of security incidents/data breaches (including the obligation to report to the supervisory authority)
X Using spam filters and regular updating *Standard included with Google Cloud Platform*	X Documented procedure to deal with security incidents
☐ Using virus scanners and regular updating *Not necessary with Google Cloud Platform*	X Involvement of X Data Protection Officer and X IT-Security Officer in security incidents and data breaches
☐ Intrusion detection system (IDS)	X Documentation of security incidents and data breaches e.g. via ticket system
☐ Intrusion Prevention System (IPS)	X Formal process and responsibilities for the post-processing of security incidents and data breaches
☐ Other measure	☐ Other measure
☐ Other measure	☐ Other measure
☐ Other measure	☐ Other measure

4.3. Data protection by default (Art. 25(2) GDPR);

Privacy by design/Privacy by default

Technical measures	Organisational measures
X No more personal data is collected than is necessary for the purpose in question	☐ Other measure
X Technical measures to facilitate the exercise of the data subject's right to withdraw consent	☐ Other measure
☐ Other measure	☐ Other measure
☐ Other measure	☐ Other measure

4.4. Supervision of contractors (outsourcing to third parties)

Measures guaranteeing that personal data processed by third party contractors can only be processed in accordance with the principal's instructions. In addition to data processing on behalf of the customer, this includes the performance of maintenance and system support work both on site and by remote maintenance. If the contractor uses service providers for the purposes of order processing, the following points shall always be regulated.

Technical measures	Organisational measures
☐ Other measure	☐ Prior examination of the safety measures taken by the contractor and their documentation
☐ Other measure	X Contractor selected with due care (especially in relation to data protection and data security)
☐ Other measure	X Conclusion of the necessary agreement for data processing or EU standard contract clauses
☐ Other measure	X Written instructions to the contractor
☐ Other measure	X Undertakings to comply with data confidentiality provided by the contractor's staff
☐ Other measure	☐ Undertaking by the contractor to appoint a data protection officer where there is an obligation to do so

☐ Other measure	☐ Agreement of effective monitoring rights with the contractor
☐ Other measure	X Regulation of the use of further subcontractors
☐ Other measure	X Guarantee that data will be destroyed after the assignment ends
☐ Other measure	X In the event of a longer term collaboration: on-going assessment of the contractor and their level of protection

Signature Customer	Signature Embrosa Melanie van Norden
Date	Date
Place	Place

Annex III

LIST OF SUB-PROCESSORS

EXPLANATION:

This annex must be completed for modules two and three in the case of separate approval of sub-processors (clause 7.7(a), option 1).

If more than 4 sub-processors are to be specified - please complete more than once.

The Controller has authorized the use of the following sub-processors:

Sub-processor Nr.: SP0001

Name: Google Cloud Platform *(including Firebase)* & Google Workspace

https://cloud.google.com/terms/sccs/eu-c2p (including Firebase https://firebase.google.com/support/privacy)

Address: Click or type here to enter the adress.

Contact person of sub-processor:

Name: Click or type here to enter the name.

Position: Click or type here to enter the position.

Contact details: Click or type here to enter the contact details.

☐ Contact person is data protection officer ☐ internal

☐ external

Description of the processing (including a clear delineation of responsibilities if multiple sub-processors are authorized):

Embrosa hosts and built her software on top of the Google Cloud Platform (including Firebase and BigQuery. Embrosa's databases store personal data on the Google Cloud Platform. And Embrosa's software, used to automatically set up and manage the hyper-local campaigns, runs on / using the Google Cloud Platform.

Firebase is a set of backend cloud computing services and application development platforms provided by Google. It hosts databases, services, authentication, and integration for a variety of applications, including Android, iOS, JavaScript, Node.js, Java, Unity, PHP, and C++

Embrosa also makes use of Google Workspace. Google Workspace is a collection of cloud computing, productivity and collaboration tools, software and products developed and marketed by Google.

Sub-processor Nr. SP0002

Name: Freshworks > Discontinued. Replaced by SP0006 Gleap GmbH

Address:

Contact person of sub-processor:

Name: Click or type here to enter the name.

Position: Click or type here to enter the position.

Contact details:

☐ Contact person is data protection officer ☐ internal

☐ external

Description of the processing (including a clear delineation of responsibilities if multiple sub-processors are authorized):

Sub-processor Nr.: SP0003

Name: MediaMeisters > Discontinued. Not replaced

Address:

Contact person of sub-processor:

Name:

Position:

Contact details:

☐ Contact person is data protection officer ☐ internal

☐ external

Description of the processing (including a clear delineation of responsibilities if multiple sub-processors are authorized):

Sub-processor Nr.: SP0004

Name: Multiply B.V. > Discontinued. Not replaced

Address:

Contact person of sub-processor:

Name:

Position:

Contact details:

☐ Contact person is data protection officer

☐ internal

☐ external

Description of the processing (including a clear delineation of responsibilities if multiple sub-processors are authorized):

Sub-processor Nr.: SP0005

Name: META (Facebook, Instagram and WhatsApp)

Address: https://www.facebook.com/business/gdpr and

https://www.whatsapp.com/legal/privacy-policy-eea

Contact person of sub-processor:

Name:

Position:

Contact details:

☐ Contact person is data protection officer ☐ internal

☐ external

Description of the processing (including a clear delineation of responsibilities if multiple sub-processors are authorized):

Embrosa creates Advertising campaigns in the advertising platform of META (to publish Ads on Instagram and Facebook). No personal data is disclosed to META. The only data that is inputted in META, when setting up an advertising campaign, is (public) name of the Company (e.g. as Adset-name or the (Company) name is included in the Ad-texts to personalize) and the address of the Company (to hyper-locally target around this location). To set up the Ads through the Embrosa software, we use the Facebook Page ID and the Instagram Page ID. So no personal data is disclosed to META.

Embrosa also handles inbound and outbound messages as part of her support and marketing service via WhatsApp.

Sub-processor Nr. SP0006

Name: Gleap

Address: Am Dorfpl. 3, 6858 Schwarzach, Austria

Contact person of sub-processor:

Name: Lukas Böhler

Position: +43 5572 401104

Contact details: privacy@gleap.io

X	Contact person is data protection officer	X internal
		X external

Description of the processing (including a clear delineation of responsibilities if multiple sub-processors are authorized):

Gleap GmbH offers its customers a bug reporting and customer feedback software for mobile applications and websites. In particular, our company offers (i) bug reporting, (ii) crash reports, (iii) live chats, (iv) features requests, (v) surveys, (vi) chat messages (direct communication), (vii) emails (same technology as surveys and chat messages), (viii) news & release notes, and (ix) a help center.

Embrosa uses the complete Gleap Suite for CRM-purposes, among which to (bulk) e-mail campaign participants about the start, finish, progress, and results of their campaign.

Embrosa uses also Gleap for Customer Support, in order to respond to customer questions through email, chat, WhatsApp, Instagram, Facebook etc.

Sub-processor Nr. SP0007

Name: Google Ads

Address: https://policies.google.com/technologies/ads

Contact person of sub-processor:

Name: Click or type here to enter the name.

Position: Click or type here to enter the position.

Contact details:

☐ Contact person is data protection officer ☐ internal

☐ external

Description of the processing (including a clear delineation of responsibilities if multiple sub-processors are authorized):

Embrosa creates Advertising campaigns in the advertising platform of Google. No personal data is disclosed to Google. The only data that is inputted in Google, when setting up an advertising campaign, is (public) Company name (e.g. as Campaign-name or Adset Name, the (Company) Name and/or (Company) Photo/Video is included in the Ad to personalize) and the location of the Company (to hyper-locally target around this location).

Sub-processor Nr. SP0008

Name: Vistar Media

Address: Danzigerbocht 45P, 1013AM Amsterdam, The Netherlands

https://www.vistarmedia.com/privacy

Contact person of sub-processor:

Name: Click or type here to enter the name.

Position: Click or type here to enter the position.

Contact details: Privacy@VistarMedia.com

Data Protection Officer, +1-833-202-5126 | 149 Fifth Avenue, Sixth Floor, New York NY 10010

☐ Contact person is data protection officer ☐ internal

☐ external

Description of the processing (including a clear delineation of responsibilities if multiple sub-processors are authorized):

Embrosa creates Advertising campaigns to be displayed on Digital Out of Home screens (LocalPanels) using the software of Vistar Media. No personal data is disclosed to Vistar Media. The only data that is inputted in Vistar Media, when setting up an advertising campaign, is (public) Company name (e.g. as Campaign-name) and/or a (Company) Photo/Video is included in the Ad to personalize) and the location of the Company (to hyper-locally target around this location).

Sub-processor Nr. SP0009

Name: Voys (Voice over IP | A phone system via the internet)

Address: Lübeckweg 2, 9723HE Groningen, The Netherlands

https://www.voys.nl/privacy-en-toegankelijkheid/

Contact person of sub-processor:

Name: Click or type here to enter the name.

Position: Click or type here to enter the position.

Contact details: security@voys.nl

☐ Contact person is data protection officer ☐ internal

☐ external

Description of the processing (including a clear delineation of responsibilities if multiple sub-processors are authorized):

Embrosa uses Voys for her inbound and outbound phone calls, including call registration. The (Company) Phone number is saved. Embrosa also uses the Voys Intelligence feature, which automatically transcribes the text from those recorded calls. In these calls and transcribed texts, (Company) Name can be recorded.

Signature Customer	Signature Embrosa Melanie van Norden
Date	Date
Place	Place

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[5] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

[6] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

[7] This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

[8] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[9] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[10] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

[11] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

[12] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[5] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

[6] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

[7] This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

[8] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[9] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[10] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

[11] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

[12] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.