Data Processing Agreement

This Data Processing Agreement (hereinafter: "DPA") forms an integral part of the main agreement(s) entered into by you (counterparty) and Easy2Meet B.V. and the general terms and conditions applicable to them. Easy2Meet B.V. is Processor (hereinafter: "Processor") of the personal data and the counterparty is the process controller (hereinafter: "Controller") for the personal data.

Processor and Controller, jointly to be referred to as "Parties",

whereas:

- Controller has access to personal data of various customers or customers of customers (hereinafter: "Data Subjects");
- Controller uses the services of Processor and/or their Easy2Meet® software for meeting management;
- Controller has personal data processed by Processor through the use of Processor's meeting software Easy2Meet®, whereby Controller designates the purpose and the means. This in the context of the agreement between the Parties (hereinafter to be referred to as: "the Main Agreement");
- Processor complies the obligations regarding security and other aspects of the legislation and regulations regarding the protection of personal data (such as the General Data Protection Regulation (hereinafter: "GDPR")), this of course to the extent that this lies within its responsibility;
- Parties, also in view of the requirement of Article 28 section 3 of the GDPR, wish to formulate in writing their rights and obligations in this DPA;
- Processor in the performance of the Main Agreement may be regarded as Processor within the meaning of Article 4, section 8, of the GDPR;
- Controller is regarded as responsible within the meaning of Article 4 section 7 of the GDPR;
- References to personal data in this DPA, personal data within the meaning of Article 4(1) of the GDPR are meant;
- The terms from the GDPR used in this DPA are the corresponding terms from the GDPR;

agree as follows:

Data Processing Agreement

Article 1. Processing

1.1. Under the terms of this DPA, Processor is processing personal data on behalf of Controller. Processing takes place exclusively within the scope of this DPA and for the purposes set out in the Main Contract. Controller shall inform Processor in writing of the purposes of processing insofar as they are not already mentioned in this Main Contract and/or can be derived from it.

1.2. Processor has no control over the purpose and means of processing personal data. Processor shall not make independent decisions about the receipt and use of the personal data, the disclosure to third parties and the duration of the storage of personal data.

Article 2. Responsibilities

2.1. Parties shall ensure compliance with applicable privacy laws and regulations.

2.2. Permitted processing will be carried out by Processor within a (semi-)automated environment.

2.3. Processor is solely responsible for the processing of personal data under this DPA, in accordance with the instructions of Controller and under the express (ultimate) responsibility of Controller. Processor is not responsible for all other processing of personal data, including but not limited to the collection of personal data by Controller, processing for purposes not reported to Processor by Controller, processing by third parties and/or other purposes. The responsibility for these processing operations rests exclusively with Controller.

2.4. Controller guarantees that the content, the use and the order to process personal data, as referred to in this DPA, is not unjustified and does not infringe any rights of third parties.

Article 3. Obligations Processor

3.1. With regard to the processing referred to in Article 1, Processor shall ensure compliance with the conditions laid down, pursuant to the GDPR, for the processing of personal data by Processor in its role.

3.2. Processor shall inform Controller, at its first request and within a reasonable period of time, of the measures taken regarding its obligations under this DPA.

3.3. Processor shall notify Controller if, in its opinion, an instruction from Controller is in breach of relevant privacy laws and regulations.

3.4. Processor shall provide Controller with the necessary cooperation when a data protection impact assessment, or prior consultation of the supervisor, should be necessary in the context of the processing.

3.5. The obligations of Processor arising from this DPA also apply to those who process personal data under the authority of Processor, including but not limited to employees, in the broadest sense of the word.

3.6. The processing takes place under the responsibility of Controller.

3.7. Processor shall only make the personal data available to those employees who need the personal data for the performance of their work or who necessarily need to take note of the personal data in the context of and for the performance of the Agreement, and shall otherwise keep it confidential, except where it is subject to different statutory obligations.

Article 4. Transferability of personal data

4.1. The personal data used when working with or in Easy2Meet® is stored in a datacenter within the European Economic Area (EEA). It should be noted that with regard to the storage of documents, it is ultimately Controller himself who stores the documents.

4.2 The personal data of Controller itself, not being for the purpose of working with Easy2Meet® but which is used to be able to provide optimal administrative services to Controller, is stored in Processor's CRM which runs on a hosted environment from the USA and to which the EU-US Privacy Shield applies.

Article 5. Engaging of third-parties or Sub-Processors

5.1. Processor uses with the approval of Controller Microsoft's Azure infrastructure for its services, which as such can be regarded as a Sub-Processor. A further explanation of the rights and obligations regarding Microsoft's services is given at https://products.office.com/nl-nl/business/office-365-trust-center-compliance.

5.2. If Processor at any time (additionally) makes use of third parties or Sub-Processors, this is done with due observance of the nature of this agreement. Prior to this, the Controller's Personal Data Officer will be informed and given the opportunity to lodge an objection; the term for this is one month after the moment for information.

Data Processing Agreement

Article 6. Security

6.1. Processor shall take appropriate technical and organizational measures to protect personal data against loss or against any form of unjustified processing (such as unauthorized access, alteration, alteration or disclosure of personal data) as referred to in Article 32 GDPR. To this end, Processor has adopted the security measures set out in Annex 1.

6.2. Processor shall be responsible for compliance with the security measures taken.

Article 7. Notification requirement for data breaches

7.1. In the event of a security and/or data breach, Processor shall inform Controller as soon as possible, but no later than within 48 hours, on the basis of which Controller shall assess whether or not to inform the supervisory authorities and/or data subjects. Processor makes every effort to ensure that the information provided is complete, correct and accurate. Notification shall be made to Controller's Personal Data Officer.

7.2. In the event of a security incident (which is understood to mean: any element and/or inadequacy in the means used by Processor for the processing of personal data that could potentially lead to a personal data breach), Processor shall do its utmost to inform Controller as soon as possible, but at the latest within 48 hours, as a result of which Controller shall decide whether or not to inform the supervisory authorities and/or data subjects. Processor makes every effort to ensure that the information provided is complete, correct and accurate. Notification shall be made to Controller's Personal Data Officer.
Processor shall take all appropriate technical and organizational measures to limit the consequences of a security incident and/or to prevent a new security incident.

7.3. Controller shall ensure that any (statutory) reporting obligations are complied with. If required by law and/or regulations, Processor shall cooperate in informing the relevant authorities and any parties involved.

7.4. The obligation to report will be handled in accordance with the procedure set out in Annex 2.

Article 8. Handling of requests from Data Subjects

8.1. In the event that a Data Subject sends a request about his personal data to Processor, Processor forwards the request to Controller. Processor may inform the Data Subject of this. Processor cooperates with Controller in handling the request. If it appears that Controller needs help from Processor for the execution of a complainant's request, this may incur costs. In that case, consultations will be held about this and if this is unavoidable for the execution, Processor will charge for this.

Data Processing Agreement

Article 9. Confidentiality

9.1. All personal data that Processor receives from Controller and/or collects itself within the framework of this DPA are subject to an obligation of confidentiality towards third parties. Processor does not use this information for any other purpose than that for which it was obtained. Unless these data are presented in such a form that they cannot be traced back to those involved - directly or indirectly - and do not contain any company confidential data, Processor will then use the aggregated and anonymized data exclusively for analysis purposes.

9.2. This obligation of confidentiality does not apply:

- to the extent that Controller has given express permission to provide the information to third parties; or
- if the provision of the information to third parties is logically necessary for the performance of the Main Contract or this DPA; and
- if there is a legal obligation to provide the information to a third party.

9.3. Processor shall keep the personal data it processes in the context of the implementation of the DPA confidential and shall take all necessary measures to ensure the confidentiality of the personal data.

9.4. Persons employed by, or working for Processor, including sub-processors and third parties, are deemed to observe confidentiality with regard to the personal data of which they (may) become aware, except to the extent that a provision laid down by, or pursuant to, the law obliges them to disclose such personal data.

9.5. If Processor is required by law to provide data, Processor shall verify the basis of the request and the identity of the applicant and inform Processor Controller immediately, prior to the provision of data. Where applicable, Controller shall receive a copy of the provided data from Processor.

Article 10. Audit

10.1. Controller has the right to carry out an audit, or have one carried out by an independent expert third party who is bound by confidentiality, in order to check compliance with all points from this DPA and everything directly related to it.

10.2. This audit only takes place after Controller has requested and assessed the similar relevant audit reports from Processor and has presented reasonable arguments to justify an audit initiated by Controller. Such an audit is justified if the similar audit reports present at Processor do not provide, or do not sufficiently provide, a definite answer on Processor's compliance with this DPA. The audit initiated by Controller takes place two weeks after the previous announcement by Controller, at most once per calendar year.

10.3. Processor participates in the audit and makes available all information reasonably relevant to the audit, including supporting data such as system logs, and employees as soon as possible and within a reasonable period of time, whereby a period of no more than two weeks is reasonable unless there is an urgent interest to the contrary.

10.4. The findings of the audit shall be assessed by the Parties in mutual consultation. As a result, changes will be made to the security system, whether or not they are implemented by one of the Parties or by both Parties jointly.
10.5. All costs of the audit shall be borne by Controller, unless it appears that Processor has failed to comply with its obligations under this DPA.

Article 11. Liability

11.1. Processor's liability is arranged according to article 82 GDPR.
11.2. When damaged is suffered by Contoller, then it will be processed as stated in article 12 of the General Terms and Conditions of Processor.
11.3. The condition for the existence of any right to compensation is always that Controller notifies Processor in writing and by registered mail of the damage as soon as possible after it becomes known. Any claim for damages by Controller expires by the mere expiry of three months after Controller has become aware of the fact that he has suffered damages.
11.4. Processor is explicitly not liable for any damage suffered by Controller as a result of a fine imposed by one of the national regulators, including the Dutch Data Protection Authority, amongst others in the context of statutory reporting obligations. Unless it has been established that Processor did not comply with the applicable laws and regulations during the processing or Processor acted outside or in violation of the legitimate instructions of Controller, or employees, sub processors or third parties engaged by it.

Article 12. Duration and termination

12.1. This DPA is established by agreeing to the Main Contract during the placing of an order.
12.2. This DPA has been entered into for the duration stipulated in the Head Agreement between the Parties and, failing that, in any event for the duration of the cooperation.
12.3. As soon as the DPA has been terminated, for whatever reason and in whatever manner, Processor gives the opportunity to download or export to Controller all personal data it holds in an Excel, CSV or PDF file in its original form or as a copy.
12.4. Personal data in the possession of Processor shall be deleted or destroyed after the statutory retention obligation and/or period has expired.
12.5. Changes to the DPA shall be notified in advance. Any objections can be submitted within one month of the announcement, after which Processor is obliged to maintain the intended change and to contact the encumbered party or parties. Only if there is a question of a proposed change actually affecting the nature of the DPA will an objection be honoured and the proposed change cannot be implemented.

Article 13. Other conditions

13.1. The DPA and its implementation are governed by Dutch law.

Data Processing Agreement

13.2. All disputes that may arise between the Parties in connection with the DPA will be submitted to the competent court in Rotterdam.

13.3. Logs and measurements made by Processor shall be regarded as conclusive evidence, subject to proof to the contrary to be provided by Controller.

13.4. In the event of conflict between different documents or their appendices, the following order of priority shall apply:

- the Main Agreement;
- The General Terms and Conditions of Processor as filed with the Chamber of Commerce in Rotterdam;
- this DPA;
- any additional conditions.

Thus made and signed,

Zwijndrecht, August 2020,

P.A. de Graaf
CEO

Data Processing Agreement

Annex 1: Specification personal data

Processor processes the following personal data within the framework of the Main Contract and by order of Controller:

In a general sense, the name and address details as referred to in the Main Contract as well as in meeting documents; in addition:

- Contact details (e-mail address and telephone number);
- Gender;
- IP address;
- Payment details;
- Login names (no passwords).

Controller warrants that the personal data described in this Attachment 1 are complete and correct and indemnifies Processor against any defects and claims resulting from incorrect display by Controller.

With respect to the processing, Processor has taken the following security measures:

- Logical access control, using two factor authentication (MFA);
- Access to Processor's database and files based on a limited set of IP addresses;
- Encryption of the database in which personal data is stored;
- Organizational measures for access security;
- Security of network connections via Transport Layer Security (TLS) technology;
- Confidentiality of employees and third parties involved.

These measures take place within the framework of ISO27001.

Data Processing Agreement

Annex 2: Procedure in the event of a security incident

A security incident is an incident in which the integrity, confidentiality or availability of the personal data is affected or threatened. Such as, but not limited to: unauthorized access, unlawful processing, accidental deletion or loss, unauthorized disclosure, or any indication that such a breach is occurring or has occurred. This concerns data that can be linked to a person, directly or indirectly, such as: name, addresses, contact details, IP or MAC addresses, unique identifying numbers (citizen service number, personnel number).

In the event of a security incident, it will be investigated whether personal data are involved and what the consequences are. A notification to the Dutch Data Protection Authority must be made in the event of any incident involving personal data, unless the data breach is unlikely to present a risk. Reporting to the Controller's Personal Data Officer must take place within 72 hours of the discovery of the data breach. In addition, a report must be made to the parties involved if the data leak is likely to involve a high risk. Controller is fully responsible for considering whether there is an obligation to report to the authority or to the person involved.

Processor shall inform Controller without delay, and no later than 24 hours after discovery of the security incident, that a security incident has occurred. Processor provides all information about the nature and impact of the security incident as well as the measures taken or to be taken.

Each security incident shall be reported to the designated Personal Data Officer of Controller.

Information that Processor provides, at least in relation to the security incident, is the following:

1) **Reporting contact details**

   Name, position, email address, phone number.

2) **Timeline**

   The infringement (completed as appropriate):

   a) took place on ..... (exact date) or between (start date of period) and (end date of period).
   b) The infringement is/is not longer continuing.
   c) The infringement was discovered on .....
   d) The infringement was reported later than 24 hours after discovery, because .....

3) **Data relating to the data breach**

   Nature of the breach.

   a) Breach of data confidentiality.
   b) Breach of data integrity.

c) Breach of data availability.

Nature of the incident.

d) The nature of the personal data security breach incident.

e) Summary of the personal data security breach incident.

4) Personal data in general

The categories of general personal data concerned (please tick several options):

a) Name.

b) Sex, date of birth and/or age.

c) Civil service number (BSN).

d) Contact details.

e) Access or identification data.

f) Financial details.

g) (Copies of) passports or other identification documents.

h) Location details.

i) Personal data relating to criminal convictions and offences or to related security measures.

j) Unknown/other, please indicate.

How many records ('data records') (if any) were affected by the breach (approximate).

5) The group of people whose personal data are involved in the data leak

Categories of people involved.

a) Employees.

b) Customers (current and potential).

c) Pupils or students.

d) Patients.

e) Minors.

f) Persons from vulnerable groups.

Description of the group of people whose personal data are involved in the infringement.

Minimum number of persons involved in the personal data breach?

Maximum number of persons involved in the personal data breach?

6) Measures taken before the data breach occurred

a) Whether, at the time the breach occurred, the personal data were encrypted, hooked or otherwise unintelligible or inaccessible to unauthorised persons

b) If the personal data were partly incomprehensible or inaccessible, which part of the data was incomprehensible or inaccessible.

c) If the personal data had been made wholly or partly incomprehensible or inaccessible, by what means.

7) Consequences of the data breach

Consequences of the breach of the confidentiality, integrity and/or availability of the data.

a) Unauthorised persons have had access to the data.
b) The data may be misused in an inappropriate or unlawful manner.
c) Incorrect, incomplete or outdated personal data may be used within your own organization.
d) Incorrect, incomplete or outdated personal data may be re-used for other purposes or transferred to other organizations.
e) An essential service may temporarily cease to be provided to data subjects.
f) An essential service can no longer be permanently provided to data subjects.
g) Other, please indicate (also).

Physical, material and non-material harm to the data subject.

h) What impact the breach may have on the privacy of the data subject.
i) Discrimination.
j) Identity theft or fraud.
k) Financial losses.
l) Damage to reputation.
m) Loss of confidentiality of personal data protected by professional secrecy.
n) Unauthorised removal of pseudonymisation.
o) Data subjects cannot exercise their rights and freedoms.
p) Data subjects are prevented from exercising control over their personal data.
q) Other consequences, please specify.

The seriousness of the possible consequences for the data subjects is estimated as follows:

- Negligible.
- Limited.
- Considerable.
- Very large.

8) Follow-up actions on the data breach

Measures to address the infringement

a) The following technical and organizational measures have been taken to address the infringement and to prevent further infringements.

International aspects

b) The infringement has/does not occur in a cross-border data processing operation; the PfA is/does not act as the lead supervisor for this processing operation.

- Yes, the following EU countries are concerned: …….
- No.

9) Other

Has everything that matters been reported?

a) Yes.
b) No, in addition the following is also reported: …….