Chapter 8: Processor agreement

PARTIES:

1. You, the customer, hereinafter referred to as the **"Processor";**
   and

2. the private limited company **Fairtual Technologies BV**, with registered offices in Belgium, 8000 Bruges, Koningin Elisabethlaan 18, represented in this matter by its director, Mr Diego Dupont, hereinafter referred to as the **"Processor"**.

CONSIDERATIONS:

I. The Controller has entered into or will enter into one or more agreements with the Processor for the provision of various services by the Processor to the Controller. This Agreement or these Agreements will hereinafter be jointly referred to as the "**Framework Agreement**".

II. When executing the Master Agreement, the Processor will process data for which the Controller is and will remain responsible. These data include personal data within the meaning of the General Data Protection Regulation (EU 2016/679), hereinafter the "**GDPR**".

III. In view of the provisions of **Article 28(3) of the GDPR**, the parties wish to lay down the conditions for the processing of these personal data in this agreement.

AGREEMENT:

1 Scope

1.1 This Agreement applies to the extent that the provision of the Services based on the Framework Agreement involves one or more of the processing operations listed in **Annexe 1**.

1.2 The processing operations set out in **Annexe 1** that take place during the provision of services are referred to below as: **"the Processing"**. The processed personal data are called: **"the Personal Data"**.

1.3 With regard to the Processing, the Controller is the party responsible for the processing and the Processor is the processor. The natural persons who actually make use of the services of Processor based on the Framework Agreement and, if applicable, their representatives, are hereinafter also referred to as "**the End Users**".

1.4 All terms used in this Agreement will have the meanings given to them in the GDPR.

1.5 The Annexes will form an integral part of this Agreement. The annexes are

Annexe 1 the Processing, the Personal Data, and the retention periods;

Annexe 2 the Subprocessors and categories of Subprocessors approved by the Controller;

Annexe 3 the technical and organisational measures of the Processor;

Annexe 4 information about a data breach.

2 Subject

2.1 The Processor undertakes to Process Personal Data only for the purposes of the activities referred to in this Processor Agreement and/or the Framework Agreement. The Processor warrants that, without the express and written permission of the Controller, it will not in any way use the Personal Data Processed under this Processing Agreement for its own purposes or the purposes of third parties, unless a legal provision applicable to the Processor requires this. In that case, the Processor will promptly notify the Controller of that legal requirement prior to the Processing, unless this legal requirement prohibits such notification for important reasons in the public interest.

2.2 The Processor will keep the Controller's Personal Data separate from (Personal) Data that it processes for itself or for third parties.

2.3 The Processor will carry out the Processing in a proper and careful manner.

3 Security measures

3.1 The Processor will take all technical and organizational security measures required from it based on the GDPR and, in particular, based on **Article 32 of the GDPR**

3.2 The Processor will provide a document listing the appropriate technical and organizational measures. This document will be enclosed to this Processor Agreement as **Annexe 3**.

4 Data breaches

4.1 The Processor will inform the Controller without unreasonable delay, but in any event within 24 hours, of any "personal data breach" as referred to in **Article 4(12) of the GDPR**. Such a breach is referred to as: "**Data breach**".

4.2 The Processor will provide the Controller, without unreasonable delay, with all the information in its possession and which is necessary to fulfil the obligations based on **Article 33 of the GDPR** and will provide all cooperation requested by the Controller. The Processor will provide the relevant information as soon as possible in a format acceptable to the Processor. Furthermore, the Processor will keep the Controller informed of any new developments concerning the Data Breach and will take all reasonable measures to remedy the Data Breach and to limit the consequences (or possible consequences) thereof as much as possible. The Processor will also take the necessary measures to prevent the recurrence of the Data Breach.

4.3 The Processor will not inform the Controller of a Data Breach if it is completely clear that the Data Breach does not pose any risk to the rights and freedoms of natural persons. If there are any doubts in this regard, the Processor will report the Data Breach to the Controller in order to enable the latter to determine whether the Data Breach must be reported. The Processor will document all breaches, including those not required to be reported to the Controller, and provide such documentation to the Controller once per quarter or sooner upon the request of the Controller. The documentation will at least contain the information referred to in **Annexe 4**.

4.4 It is the sole responsibility of the Controller to determine whether a Data Breach detected at the Processor should be reported to the competent authority and/or to the data subjects.

5 Engagement of Subprocessors

5.1 The Processor has the right to engage third parties as Subprocessors for the Processing without the prior written permission of the Controller.

5.2 The Processor will ensure that the third party (parties) concerned enter(s) into an agreement based on which this/these party/parties must observe at least the same legal obligations as the Processor.

5.3 The Processor will inform the Controller of the Subprocessors it engages. The Controller may object to additions or substitutions with respect to the Processor's Subprocessors.

5.4 In any event, the Controller hereby grants permission for the engagement of the Subprocessors and/or categories of Subprocessors listed in **Annexe 2**.

6 Duty of confidentiality

6.1 The Processor will keep the Personal Data secret. The Processor will ensure that the Personal Data are not directly or indirectly made available to third parties. Third parties also include the Processor's staff insofar as it is not necessary for them to have knowledge of the Personal Data. This prohibition does not apply if this agreement provides otherwise and/or insofar as a statutory regulation or judgement requires disclosure.

6.2 The Processor will ensure that persons, not limited to employees, who participate in the Processing at the Processor are bound by a confidentiality obligation in relation to the Personal Data.

6.3 The Processor will inform the Controller of any request to inspect, provide, or otherwise retrieve and communicate the Personal Data in violation of the confidentiality obligation set out in this article.

7 Retention periods and deletion

7.1 The Controller is responsible for determining the retention periods in relation to the Personal Data. Insofar as the Personal Data are under the Controller's control, it will delete these itself in a timely manner.

7.2 The Processor will delete the Personal Data within thirty days of the end of the Framework Agreement or, at the Controller's choice, transfer these to the Controller, unless the Personal Data must be retained for a longer period, such as in the context of the Processor's legal or other obligations, or if the Controller requests that the Personal Data be retained for a longer period of time and the Processor and Controller agree on the costs and other conditions of this longer retention, the latter without prejudice to the Controller's responsibility to observe the statutory retention periods. Any transfer to the Controller will be at the Controller's expense.

7.3 At the Controller's request, the Processor will declare that the deletion referred to in the previous paragraph has taken place. The Controller may, at its own expense, have an inspection carried out to determine whether this has indeed taken place. **Article 10** of this Agreement will apply to such an inspection. To the extent necessary, the Processor will notify all the Subprocessors involved in the processing of the Personal Data of the termination of the Framework Agreement and will instruct them to act as provided herein.

7.4 Unless the parties agree otherwise, the Controller will arrange for a backup of the Personal Data.

8 Rights of the data subjects

8.1 If the Controller has access to the Personal Data itself, it will comply with all the requests from the data subjects regarding the Personal Data. The Processor will promptly communicate any requests received by the Controller to the Processor, who will be responsible for handling the request.

8.2 The Processor will provide its full and timely cooperation to the Controller only to the extent that the provisions of the preceding paragraph are not possible, in order to:

(i) following the approval of and based on the instructions of the Controller, allow the data subjects to inspect the Personal Data relating to them,

(ii) Delete or correct personal data,

(iii) demonstrate that the Personal Data have been deleted or corrected if these are incorrect (or, if the Controller does not agree that the Personal Data are incorrect, record the fact that the data subject considers his/her Personal Data incorrect)

(iv) to provide the Personal Data in question to the Controller or to a third party designated by the Controller in a structured, common, and machine-readable format, and

(v) to otherwise enable the Controller to comply with its obligations based on the GDRP or any other applicable act related to the processing of Personal Data.

8.3 The costs of and the requirements for the cooperation referred to in the **previous paragraph** will be determined jointly by the parties. In the absence of an agreement to this effect, the costs will be borne by the Controller.

9 Liability

9.1 The Processor will be liable vis-à-vis the Controller for all damages and costs incurred by the Controller as a result of the Processor's attributable failure to comply with its obligations under this Agreement, including but not limited to damage caused by the Processor's failure to comply with obligations of the GDPR specifically relevant to the Processor or if the Controller's lawful instructions were violated.

9.2 The Processor will indemnify the Controller against all third-party claims resulting from an imputable failure by the Processor to perform its obligations vis-à-vis the Controller under this agreement.

9.3 Without prejudice to the provisions of this Article 9, the liability regulations laid down in the Framework Agreement will apply in full.

10 Check

10.1 The Controller is entitled to verify compliance with the provisions of this agreement at its own expense when there is reasonable cause to do so, but at least once per year, or to have this verified by an independent registered accountant or registered computer specialist.

10.2 If this audit shows that the Processor has not or has not properly complied with this Agreement and/or applicable legal provisions governing the Processing of Personal Data, the Processor will bear the costs of the investigation. The Processor will also remedy the shortcomings without delay after becoming aware of them. This is without prejudice to the other rights of the Controller.

10.3 The Processor will make all the information necessary to demonstrate compliance with the obligations of **Article 28 GDPR** available to the Controller. If the third party engaged by the Controller gives an instruction that violates the GDPR, such at the discretion of the Processor opinion, the Processor will immediately notify the Controller.

10.4 The Controller's investigation will always be limited to the Processor's systems used for the Processing. The Controller will keep the information found in the investigation confidential and will only use it to verify the Processor's compliance with its obligations under this Agreement and will delete the information or parts of it as soon as it can. The Controller warrants that any third parties engaged will also assume these obligations.

The Processor will carry out periodic security checks himself, or have them carried out, and will provide an annual summary of the results of these checks, which will at least include an overview of the risks as well as the measures for mitigating and resolving them.

11 Processing of Personal Data outside the European Economic Area

11.1 The transfer of Personal Data by the Processor outside of the European Economic Area is only permitted in compliance with the applicable legal obligations.

12 Other provisions

12.1 Amendments to this Agreement will only be valid if agreed in writing between the parties.

12.2 The Parties will amend this Agreement to reflect amended or supplemented regulations, additional instructions from the relevant authorities, and evolving understanding of the application of the GDPR (for example, through, but not limited to, case law or reports), the introduction of standard provisions and/or other events or insights that necessitate such amendment.

12.3 This agreement will last for the duration of the Framework Agreement. The provisions of this Agreement will remain in force to the extent necessary to settle this Agreement and to the extent intended to survive the termination of this Agreement. The latter category of provisions includes, but is not limited to, the provisions on confidentiality and disputes.

12.4 This agreement prevails over all other agreements between the Controller and the Processor.

12.5 This agreement is governed exclusively by the laws of Belgium.

12.6 The parties will exclusively submit their disputes related to this agreement to the Court of Bruges.

_____

By:	By:
On behalf of: **Fairtual Technologies BV**	On behalf of:
On:	On:
In:	In:

Annexe 1

Processing of personal data and retention periods

Annexes 1 and 2 must be filled out as completely as possible by the controller

This Annexe is part of the Processor Agreement and must be initialled by the parties.

I. The Personal Data that parties expect to process:

Description of the personal data processed under this agreement, such as the data described below. Please complete]

- o ……
- o ……
- o ……
- o ……
- o ……
- o ……
- o ……
- o ……
- o ……
- o ……
- o ……

II. The nature, use, and purpose of the processing of Personal Data:

Description of what happens with the Personal Data (e.g., storage in a file, emailing, etc.), the purpose of the processing (e.g., marketing, customer acquisition, contract performance), and what means are used (e.g., CRM software)]

……
……
……
……
……
……
……
……
……

III. The categories of Data Subjects to which the Personal Data relate

Description of the categories of Data Subjects, e.g. website visitors, subscribers, suppliers, children, employees].

……
……
……
……
……
……
……

……
……

IV. The periods of use and retention of the (different types of) Personal Data:

Description of the periods of use and retention to be observed by the processor]

……
……
……
……
……
……
……
……
……

Annexe 2

Subprocessors/categories of Subprocessors

This Annexe is part of the Processor Agreement and must be initialled by the parties.

This annexe contains an overview of the Subprocessors mentioned in Article 5.4 of this Agreement.

Subprocessors:

Name of subprocessor	**Address**	**Contact details**	**Goal of the subprocessor**
C Bloom Comm. V.	Blauwvoetstraat 49 - 8310 Assebroek	info@cbloom.be MOBILE PHONE:+32478211899 BE0518.858.245	3D design
Sliced Comm. V.	Watermolenstraat 23 9230 Wetteren	info@sliced.be MOBILE PHONE:+32496660979 BE0739734272	IT - development
Combell NV	Skaldenstraat 121, 9042 Ghent	administratie@combell.com VAT: BE 0541.977.701	hosting
Whereby AS	Gate 1, No. 107 6700 Maloy, Norway	pro@whereby.com	Video meetings
tawk.to inc.	187 East Warm Springs Rd, SB298 Las Vegas, NV, 89119	support@tawk.to	Written chat booths
Chatwee Sp.	Piotrkowska 4, 62-610 Sompolno, Poland	VAT ID: PL6652990463 https://chatwee.com/	Written Chat (Network Cafe)

FAIRTUAL TECHNOLOGIES BV

Annexe 3

Security measures of the Processor

The organization monitors legislation and case law related to the GDPR at regular intervals.

Chapter	Subject	Status
Security policy and information security organisation	Data Protection: A DPO has been appointed who is responsible for coordinating, advising, monitoring, and raising awareness related to data protection procedures and guidelines. This person will receive periodic refresher training so that his/her knowledge and expertise remains up to date.	A DPO has been appointed with the skills necessary to perform his/her duties. The DPO has a clear job description and no conflicts of interest can arise from other tasks that the DPO performs within the organization. Sufficient resources are available and sufficient time is spent on organizing information security with respect to the processing of personal data. There is an active decision-making platform (DPO + project team) that meets and makes decisions on a regular basis. There is also clear support from the management to start the implementation of data protection within the organization.
	Security Responsibilities: Formal data protection policies have been approved and are known to staff. Data protection responsibilities are assigned internally.	There is a general information security policy regarding the processing of personal data, which was/is communicated both internally and externally and which is reviewed regularly. There is active support from the management to the freelancers with whom the company cooperates concerning compliance with the general information security policy for the processing of personal data.
	Risk Management: A formal risk analysis was carried out, based on which data protection measures were drawn up. This process will be repeated periodically.	A risk analysis has been and is regularly carried out to assess the risks involved in the loss, unlawful transfer, modification, and the like of personal data. The cost of taking technical and organisational measures in relation to the risks of possible breaches and their impact on the rights and freedoms of data subjects has been and will continue to be assessed on a regular basis. Technical and organisational measures have been and will continue to be taken on a regular basis to avoid risks that could affect the rights and freedom of data subjects.
Safe staff policy	Confidentiality obligations: Employees are subject to a confidentiality obligation when processing personal data. This obligation is recorded in the employment contract or in the work regulations.	The Processor does not employ any staff. A confidentiality agreement was signed with all freelancers. Internal disciplinary measures are in place for violations involving the handling of personal data. The way in which employees handle personal data is checked on a regular basis.
	Raising awareness: Employees are aware of the importance of data protection and will follow the necessary procedures when processing personal data. This raising of awareness will be repeated periodically	Each freelancer who works with the Processor has attended various awareness training courses on both GDPR and cybersecurity.
	Start and end of employment: The access rights of the various employees are terminated at the end of the cooperation, so that no unauthorised persons can gain access to the personal data.	Internal transfers of employees who process or will process personal data are considered. Access rights and other rights will be reviewed and adjusted as appropriate.
Inventory of company resources	Inventory of company resources An inventory is kept of all information processing systems that are used by the employees.	A clear distinction is made at the organisational level between personal data, anonymous data, encrypted data, and sensitive data.

Cryptography	Business resources: All information processing systems used to process the Controller's information are appropriately encrypted.	There is a policy on the use of encryption, which is aligned with the risk analysis to protect the confidentiality, authenticity and/or integrity of personal data. The organization has developed a policy to protect the lifespan of cryptographic keys during their entire life cycle.
	Transfer of information: All confidential data of the controller will only be transferred with the help of a secure connection.	Secure connections are always used.
Physical security	Physical access: Access to the premises where personal data are processed is only possible for identified and authorised persons.	Appropriate security measures are taken regarding physical security of premises and buildings. Any potential damage (fire, water...) is taken into account. Consideration is given to the security of equipment, cabling, and supporting facilities to prevent loss, damage, theft, and unwanted alteration of personal data. Particular attention is paid to equipment located or used outside the premises of the organization.
Access control	Access Policy: The rights of each employee will be limited according to the need-to-know principle. More access than initially necessary will only be possible after formal approval and if there is a valid reason for this.	There is an updated and documented access policy, which clearly states who has access to which personal data. Data classification is taken into account here. A person has been appointed to handle requests related to access rights. This person is different from the person who grants, adapts, or deletes access rights in the systems at a technical level. Appropriate security measures are in place for access to data (such as password protection). There is separation of duties to prevent one person from having all the rights.
	Access Authorization: There is an appropriate authorization system to access sensitive information. Each individual will have a unique ID for logging in.	
	Authentication: A strong authentication system has been implemented for user authentication. If access to sensitive personal data is possible through the Internet, multi-factor authentication must be used.	
	Network Access: A system is in place that provides a reasonable level of assurance that access to the network is appropriately protected (such as firewalls, security provisions, etc.).	Network security (firewall, Wi-Fi...) is part of the information security plan.
Operational Security	Backup: Backups of personal data are made periodically. These backups will be kept encrypted at an external location.	A suitable backup policy is in place, which is tested and monitored regularly to ensure adequate recovery after damage, loss, theft, and unwanted alteration of personal data. There is a policy on the use of encryption, which is aligned with the risk analysis to protect the confidentiality, authenticity and/or integrity of personal data. The organization has developed a policy to protect the lifespan of cryptographic keys during their entire life cycle.
	Security updates: Security updates and security patches are monitored and installed systematically.	There is updated protection against malware. There is sufficient awareness among system users and end-users. Security updates are performed regularly.
Protection of communication	Transfer over networks: All personal data transmitted through public or internal channels or networks will be appropriately encrypted.	There is an email and Internet policy (transport) paying special attention to the use of personal data in emails.
Supplier relations	Selection of Subprocessors/Subcontractors: An appropriate selection process is used in the selection of subprocessors/subcontractors, as part of which the security of personal data is assessed. Only parties that meet the current standards in the field of information security and	The security efforts of the information systems of subprocessors/subcontractors are checked at the time of purchase. Security requirements are also monitored when developing new information systems or when expanding existing information systems (applications, services, IT resources, or other information processing components...).

	data protection will be used for the processing of personal data.	
	Contractual Obligations: A processing agreement is in place with all potential suppliers that will process personal data. This agreement contains all the mandatory provisions and will be signed.	Legally approved processor agreements are in place with external processors. Processor agreements are checked for the security of personal data. The processor agreements contain sufficient guarantees that the (sub)processor(s) process(es) personal data in compliance with the GDPR. These (sub)processor(s) are monitored in order to ensure compliance with the GDPR.
Information Security Incident Management	Incident management: There is an internal procedure that ensures that possible security breaches are also reported and subsequently dealt with by the responsible people. This procedure was also clearly communicated internally. All possible security breaches are recorded in a central location.	Incidents can be detected, dealt with, and reported based on documented procedures. The DPO is notified immediately in case of incidents. The DPO knows all the weaknesses that can lead to incidents, as well as the solutions that can avoid risks. Responsibilities are clear in the event of an incident.
	Notification of incidents: In the event of a possible security incident affecting the confidentiality, integrity, or availability of personal data, the necessary steps will be taken to ensure that the controller is informed in a timely and adequate manner .	The organisation is able to guarantee the continuity and availability of personal data at all times based on the results of a risk analysis. There is a business continuity plan. The organization provides sufficient redundancy (= event prevention) within the data processing services to ensure the availability of personal data. Additional data protection risks due to redundancy are taken into account.
Business continuity	Emergency repair: An appropriate system is in place to guarantee the availability and integrity of data in the event of a failure.	There is a privacy statement that complies with the GDPR and contains the following information: • The Controller's identity • The purposes for which the data will be processed • The personal data processed for each objective • The statutory ground for the data processing • The retention periods • Whether the data is exchanged outside the European Union • The possibility for the data subject to lodge a complaint with the Data Protection Authority if he/she believes that his/her personal data are being processed incorrectly • The rights of the data subjects • The technical and organizational measures taken by the organization to protect personal data There is a register of the processing activities that complies with the GDPR legislation. This register contains: • the name and contact details of the (joint) controller, of the controller's representative and/or of the data protection officer • the purpose of the processing • a description of the categories of data subjects • a description of the categories of personal data • the categories of recipients to whom the personal data have been or will be disclosed • recipients in third countries or international organisations • retention periods • a general description of the technical and organisational security measures • transfers of personal data to a third country or an international organisation and, where appropriate, the documentation of appropriate safeguards Requests from data subjects regarding their rights can be met: • The rights of data subjects are made available to data subjects in a concise, transparent, understandable, and easily accessible form and in clear and simple language • The organization complies with the right to information. • The organization complies with the right of inspection. • The organization complies with the right to correction.

		• The organisation complies with the right to erasure/right to be forgotten. • The organization complies with the fact that the scope of personal data that is processed is limited. • The organisation will take the right to data portability into account. • The organization complies with the right to object. • The organisation takes the data subject's right not to be subject to automated decision making, including profiling, into account The organization has defined the statutory grounds for each processing operation. Where appropriate, the data subject's permission for the processing of his/her personal data will be sought and a voluntary choice will be offered, in which the data subject may explicitly give his/her permission (opt-in). Permission is obtained by means of an active action and the data subject can withdraw his/her permission at any time in a manner that is just as simple as the opt-in process. All permission obtained for the processing of personal data is verifiable (logging...). No data of children are processed. A DPIA or a Data Protection Impact Assessment was conducted prior to all processing operations when a high privacy risk is clear. The organization regularly monitors legislation and case law regarding the GDPR
Compliance	Compliance: The controller can request proof of the fulfilment of the requirements for compliance.	

Annexe 4

Information in the event of a data breach

The Processor will provide all the information that the Controller deems necessary to be able to assess the Data Breach or incident. In doing so, the Processor will provide at least the following information to the Controller:

- what is the (alleged) cause of the Data Breach or incident;
- what is the consequence (as known and/or expected at that time);
- what is the proposed solution;
- the contact details for following up on the report;
- (an estimate of) the number of persons whose data are involved in the Data Breach or incident;
- a description of the category of data subjects involved in the Data Breach or incident;
- the type or types of Personal Data involved in the Data Breach or incident;
- the date/period on/during which the Data Breach or incident occurred;
- the date and time on/at which the Data Breach or incident became known to the Processor or to a third party or subprocessor engaged by it;
- whether the data have been encrypted, hashed, or made otherwise inaccessible to unauthorised persons;
- what measures have been taken to end the Data Breach or incident and to mitigate the consequences of the breach.