General terms and conditions

01/01/2024

"All our services are performed in accordance with the General Terms and Conditions. These are the mutual agreements we make. Because good agreements make good friends".

Inhoud

Chapter 1: Who or what is Threedee World?

Threedee World BV is a 100% Belgian company. Our shareholders are Belgians, born and raised and we do not have any interference from other parties.

Our mission:

We start from a mission. A mission to market virtual worlds, events and showrooms. We believe in a hybrid future where live (physical) and virtual (digital) can go hand in hand and reinforce each other. We also believe that digital communication is undeniably part of the communication mix. Transparency, customer-friendliness and flexibility are things we value highly. How do we do that? With clear and useful advice, clear communication and all that With a smile. Because that's how we make the difference.

Our Company Details:

THREEDEE WORLD BV – Leonardo da Vincilaan 19A 8 – 1831 Diegem (België) – KBO 0726.840.893.

We are satisfied customers of Belfius Bank and Insurance under the account number:

IBAN: BE81 0689 4390 6724

Our team - our specialists:
We work with a team of specialists. Specialists that we dedicate to our clients to make their project a success.

Chapter 2: Our advance communication: focus on clarity

2.1 Our prices will always be communicated in advance in as complete and clear a manner as possible. You will always know in advance how much you will pay, except for specific custom work.

2.2 We work with clear quotations and price agreements so that the price is clear and transparent in advance. Quotations are always valid for 30 days.

2.3 An offer (in the form of a quotation) is considered accepted after explicit or implicit acceptance by you. This acceptance also means that you have read and agree to our Terms and Conditions (in its entirety). We always ask you to sign the quotation(s) digitally. This saves everyone a lot of work and paper.

2.4 Explicit acceptance means that you clearly state in no uncertain terms that you agree to the offer (the quotation), and that the work may begin. With an implicit acceptance, you perform some action from which it can be inferred that you agree to the offer (for example, forwarding certain items we need to begin work on a job, or paying a deposit).

2.5 As soon as an assignment is accepted, the activities are started. A project is created and planned, the administrative framework is set up, internal briefings take place, etc. After this acceptance, you can no longer cancel free of charge. However, if you wish to cancel, you can. If you cancel more than 1 month before the planned delivery, you pay 50% of the total costs (even if certain works or other matters have not yet been carried out). If you cancel less than 1 month before the scheduled delivery, you pay 75% of the total costs (even if certain works or other matters have not yet been carried out).

2.6 Deadlines are important. We will always clearly agree the deadlines associated with assignments with you as well. We strive to meet 100% of our deadlines.

2.7 Since communication is important, we find it necessary to make clear agreements about this (deadlines). Thus, each project is managed by our Customer Success Manager(s). The CSM is the key figure who manages the activities of our team. Team members other than the CSM are therefore best not contacted directly by you so that they can focus on their jobs. If you contact one of those employees directly, the time spent on this will be charged at an hourly rate. So keep this in mind. On the other hand, if one of the employees contacts you directly, this does not apply (as far as these contacts are concerned).

Chapter 3: The Costs - billing and payments

3.1 Fixed costs

For most cases, we work with "flat fees." These can also be free of charge. This way, you as a customer know well what you are starting with and can start budgeting your project perfectly.

The fixed costs (along with any other costs) are listed on the quote and are necessarily unchangeable.

3.2 Variable costs

We also have "variable costs." The amount of our variable costs depend on the amount of the fixed costs. We distinguish 2 variable costs.

First, there are the costs related to project management. This is the support our people offer you during the preparation and possible live days of your event.

We also apply a variable eco-premium. Threedee World is an ecological company that is climate conscious. To offset our organization's carbon footprint, we will undertake some climate promoting initiatives. We will share the cost of these with our customers. Consequently, we apply a variable cost of 25% on any ticket price you charge when visitors wish to attend your event. This will appear on your final invoice.

3.3 Hourly rates - customization (or other)

In cases where we work on an hourly rate such as customization for example, we charge an hourly rate of 85 EUR excl. VAT.

For example, if you request us to customize a booth or develop additional functionality, we will initially estimate the number of hours (or days) we will need for this development(s). You will then receive a quote, which will include a number of hours (or days or a fixed rate). Please note that this is always an estimate. This means that there is either more work, or less work and therefore more or less can be invoiced respectively.

Our people are now able to make correct estimates, but it sometimes happens that our customers ask for extra adjustments or do not deliver the things we need for the development.

3.4 Relocation costs

As an ecological company, we don't particularly like to travel. Travel also prevents us from working in the office, so we charge travel expenses at 1 € / km (including travel time). Since we cannot take into account any travel "to be made" during the quotation phase, travel expenses are not included in the quotation. However, they are invoiced afterwards.

3.5 Billing

We always invoice (in case payment is due) in at least 3 times.

A first invoice of 40% of the approved quote amount is invoiced within the week after the quote is signed.

The second invoice shall be sent at least 4 weeks prior to the start of the event or delivery of the project and shall be 30% of the approved bid amount.

The third invoice will be sent at least 2 weeks before the start of the event or project delivery and will be 30% (or the balance) of the approved bid amount.

If there are subsequent items to settle, this invoice will be sent immediately following the event or completed project.

3.5 Payments

The standard payment term is 14 days from invoice date. If you wish to obtain an extended payment term, prior written approval is required. Reference to your own payment terms or general conditions will not be accepted.

3.6 What if you have not paid within the payment period mentioned under 3.5

Good agreements make the best friends, including with us. We make every effort to make your event/project a success. The respect we ask in return is proper payment of our invoices.

If an invoice was not paid by the due date (invoice date + 14 days), you will receive a friendly reminder asking you to pay the invoice within 7 days.

If you have not paid 7 days later, you will receive a second reminder on the 21st day after the invoice date. This reminder will ask you to pay the invoice within 7 days.

If on the 28th day you still have not paid, we will assume that it is not an oversight. The work will then be halted until you have paid all outstanding invoices. If any other invoices are to be made, they will also be made out and are due immediately, notwithstanding any work or other matters not yet performed.

We would like to make three remarks:

- Don't wait until the due date has passed and you receive a reminder. Conversely, you should also expect us to be proactive and stick to agreements / deadlines;
- In any case, make sure that the first 3 invoices are paid before the start of the event or delivery of the project. We will keep the digital doors closed in case of outstanding invoices;
- Have an unexpected problem paying an invoice? Then talk to us! We are people and entrepreneurs among ourselves and always find a solution.

If an invoice remains outstanding for more than 45 days, we will declare you in default. A conventional damage clause equal to 10% of the outstanding amount will then be charged, as well as interest of 1% per started month.

3.5 What if you disagree with an invoice received?

We try to avoid them, of course, but occasionally you will have a complaint. No problem of course! Just send a motivated and clear email to billing@threedee.world, within 8 days of noticing the problem, to inform us. We will immediately do everything possible to solve the problem.

Just keep in mind that making such a complaint does not mean the suspension of your payment obligations!

Chapter 4: Our Approach: Focus on the Customer

4.1 With every job, we keep one clear goal in mind: a satisfied customer. Accordingly, we employ all possible means to achieve that goal. We always do this at our own discretion and rely on our own experience and expertise to do so in a considered manner. This means that we may also call upon experts not associated with us when we believe it would be appropriate to do so.

4.2 We love innovation and digitalization. Thus, we also use innovative and digital applications to make certain processes faster or easier. We expect you to accept and understand the use of the applications we use.

4.3 We go for a satisfied customer. However, we do not believe in cooperation where everything comes from one side. We always try to work together with you toward the desired result. This means that we also count on the cooperation of you.

4.4 Due to the specific nature of our business, all commitments made between us and you must be viewed as best efforts commitments. It is impossible for us, due to the nature of our business, to enter into obligations of result.

To clarify: A best efforts or means commitment is a commitment whereby the executor of the works guarantees to the client that he will use all possible and available means to achieve a certain result. With a guarantee commitment or result commitment, the assignment can only be considered successful if the predefined result has been effectively achieved (this is possible, for example, in the construction of a house, but not in our activities).

4.6 It is always our goal to build a healthy and lasting relationship with you. However, should it appear that due to certain circumstances further cooperation has become impossible, we have the right to unilaterally terminate the agreement..

4.7 The intellectual rights applicable to all items developed by us always remain our integral property. You always receive a non-exclusive and non-transferable right of use. This therefore also means that you may only use these items for the purposes communicated in advance.

4.8 We take responsibility. We accept liability for any culpable major or frequent minor error that has occurred to us in the performance of paid assignments.

If you believe you have identified such an error, please email contact@threedee.world within 8 days of the date of such identification. We will then make every effort to correct this error within a reasonable period of time.

Should we not succeed in correcting our mistake, we accept our liability for the damage which is a direct consequence of this mistake. However, we can obviously not be held liable for any non-direct damages such as, for example, consequential damages, loss of profit or increase in overhead costs (this enumeration is obviously not exhaustive).

The damages for which we can be held liable can never exceed:

- The total amount invoiced excluding VAT (which has been paid);
- The amount for which we are insured according to our professional liability policy (Axa - No. 010.730.530.920 up to an amount of 125,000 EUR).

Since we do not shirk our responsibility, we expect the same from you. As a customer of ours, you will always take the necessary measures to indemnify us against damages that are due to your own shortcomings. In particular, you will have to comply with the deadlines we set for you.

4.9 Of course, force majeure can never be ruled out. Neither for you nor for ourselves. This means that if an external cause arises which makes the further execution of the agreement temporarily impossible for one of the parties, the agreement can be suspended for a period of maximum 90 days. If the force majeure still exists after this period, the contract may be terminated permanently.

When such a circumstance occurs, the party who is prevented from doing so must inform the other party in writing of the nature of the force majeure, within 8 days from the first day on which the force majeure was established.

Chapter 5: And Beyond that…

5.1 Threedee World BV is a Belgian company. This means that only Belgian law applies to agreements entered into by us. Disputes will be settled through Arbitration. This means that all disputes that may arise as a result of the present agreement or agreements that may be the result thereof, will be settled by an arbitral tribunal, consisting of one or three independent and impartial arbitrators. Failing agreement between the parties, the appointment and/or replacement shall be made by the List Administrator. The arbitral tribunal shall organize the conduct of the proceedings and estimate the (provision for the) arbitration costs. This clause supersedes all contrary stipulations of jurisdiction.

5.2 These General Terms and Conditions apply exclusively to any contract entered into by us. The existence of additional or different terms and conditions of a contracting party other than ourselves is expressly excluded. Deviations from these General Terms and Conditions are only possible if both parties have stipulated this in writing in advance..

5.3 If any provision of these General Terms and Conditions should prove to be void, this does not mean that the entire General Terms and Conditions are void. The provisions not affected by nullity therefore retain their full effect and application.

5.4 We are entitled to engage specialized third parties in the performance of our assignments, and may assign obligations arising from agreements we have entered into to such third parties at our discretion.

5.5 Once an agreement is established, we have the right to refer to the existence (and content) of the agreement in the context of our commercial and promotional activities.

In such references, we may use protected and non-protected trade names and signs of you or other users of our platforms. Of course, under no circumstances will sensitive information of you or users of our platforms be made public. You will notify third parties (exhibitors, speakers or other stakeholders) of this and let us know if anyone objects.

5.6 As previously mentioned, we are a company that works with both internal and external collaborators (both employees and freelancers - whether partners or not). Our charges list the hourly rates we charge. These hourly rates are rates that apply if we are the contracting party. We always agree with you that you will not contract directly with our staff. Should you do so (be invoiced directly by one of our employees), we will charge you an outsourcing fee equal to 35% of the rate you paid (or were charged) to or from this employee. You get the picture…

Chapter 6: Acceptable user policies for our platforms

"We live in hellish times when it comes to cyber security. Hence, we like to make agreements about how both you and your visitors are expected to interact with our platforms. What can and cannot be done, what is allowed and not allowed, you will read below. Of course we also count on your common sense".

-> it is important that you clearly communicate this policy to platform users.

6.1. Introduction

1.1 This policy for acceptable use of our platforms (the "Policy") sets forth the rules governing:

(a) the use of the website hosting the Event, any follow-on website, and the services available on that website or any follow-on website (the "Platforms"); and

(b) the transmission, storage and processing of content by you, or by any person on your behalf, using the Platforms ("Content").

1.2 References in this policy to "you" are to each customer for the Platforms and each individual user of the Platforms and "your" should be interpreted accordingly; and references in this policy to "us" are to Threedee World (and "we" and "our" should be interpreted accordingly).

1.3 By using the platforms, you agree to the rules set forth in this policy.

1.4 You should additionally ask your users (the stakeholders, such as visitors, exhibitors, speakers, etc.) for their express consent to the terms of this policy before uploading or submitting any content or otherwise using the platforms.

1.5 You must be at least 18 years old to use the platforms; and by using the platforms, you warrant to us that you are at least 18 years old. That seems clear to us...

2. General rules of use

2.1 You may not use the Platforms in any manner that causes, or is likely to cause, damage to the Platforms or impair their availability or accessibility.

2.2 You may not use the platforms:

(a) in any manner that is unlawful, fraudulent, deceptive, competitive or harmful; or

(b) in connection with any unlawful, fraudulent, deceptive or harmful purpose or activity.

2.3 You must ensure that all content complies with the provisions of this policy.

3. Unauthorized content

3.1 The content must not be illegal or unlawful, must not infringe the legal rights of any person and must not be likely to give rise to legal action against any person (in any case in any jurisdiction and under any applicable law).

3.2 Content, and the use of content by us in any way authorized, may not be:

(a) be defamatory or maliciously false;

(b) be obscene or indecent;

(c) infringe any copyright, moral right, database right, trademark right,

(d) design right, passive right or other intellectual property right;

(e) infringe any right of trust, right of privacy or right under the

(f) data protection laws;

g) e) constitute negligent advice or contain a negligent statement;

(h) (f) constitute an incitement to commit a crime, instructions to commit a crime, or the

(i) constitute promotion of criminal activity;

(j) be in contempt of court, or in violation of a court order;

(k) constitute a violation of racial or religious hatred or discrimination laws;

(l) are profane;

(m) be competitive to us or our platform;

(n) violate state secrets laws; or

(o) constitute a breach of a contractual obligation to any person.

3.3 You must ensure that the content is not and has never been the subject of any threatening or actual legal action or other similar complaint.

4. Graphic material

4.1 Content must be appropriate for all persons who have or can access the content in question.

4.2 Content must not depict violence in an explicit, graphic or senseless manner.

4.3 Content must not be pornographic or sexually explicit.

5. Factual accuracy

5.1 Content must not be untrue, false, inaccurate or misleading.

5.2 Statements of fact in Content and relating to persons (legal or natural) must be truthful; and opinions in Content and relating to persons (legal or natural) must be reasonable, fairly held and indicate the basis of the opinion.

6. Negative opinion

6.1 The Content may not consist of or include legal, financial, investment, tax, accounting, medical or other professional advice, and you may not use the Platforms to provide any legal, financial, investment, tax, accounting, medical or other professional advice service.

6.2 The Content may not consist of advice, instructions or other information that can be followed and which, if followed, could cause death, illness or bodily injury, property damage or any other loss or damage.

7. Etiquette

7.1 Content must be appropriate, civil, tasteful and in accordance with generally accepted standards of etiquette and conduct on the Internet.

7.2 Content must not be offensive, deceptive, threatening, abusive, threatening, hateful, discriminatory or inflammatory.

7.3 Content must not cause annoyance, inconvenience or unnecessary anxiety.

7.4 You must not use the Platforms to send hostile communications or communications intended to offend, including any such communications directed at a particular person or group of people.

7.5 You may not use the Platforms to intentionally upset or offend others.

7.6 You must not unnecessarily flood the Platforms with material relating to a particular subject or area of expertise, either alone or with others.

7.7 You must ensure that content does not duplicate other content available through the Platforms.

7.8 You must ensure that content is appropriately categorized.

7.9 You must use appropriate and informative titles for all Content.

7.10 You must be courteous and polite to other users of the Platforms at all times.

8. Marketing en spam

8.1 You may not, without our written consent, use the Platforms for any purpose related to the marketing, advertising, promotion, sale or delivery of any product, service or commercial offering competitive to us.

8.2 Content may not constitute or contain spam, and you may not use the Platforms to store or transmit spam - which for these purposes includes all unlawful marketing communications and unsolicited commercial communications.

8.3 You may not send spam or other marketing communications to any person using an email address or other contact information made available through the Platforms or that you find when using the Platforms.

8.4 You may not use the Platforms to promote, host or operate chain letters, Ponzi schemes, pyramid schemes, matrix programs, multi-level marketing schemes, "get rich quick" schemes or similar letters, schemes or programs.

8.5 You may not use the Platforms in a manner that may result in the blacklisting of our IP addresses.

9. Regulated companies

9.1 You may not use the Platforms for any purpose related to gambling, gaming, betting, lotteries, sweepstakes, prize competitions or any other gambling related activity.

9.2 You may not use the Platforms for any purpose related to the offering for sale, sale or distribution of drugs or pharmaceutical products.

9.3 You may not use the Platforms for any purpose related to the offering for sale, sale or distribution of knives, guns or other weapons.

10. Monitoring

10.1 You acknowledge that we may actively monitor the content and use of the Platforms.

11. Data mining

11.1 You may not conduct any systematic or automated data scraping, data mining, data extraction or collection or other systematic or automated data collection activities through or in connection with the Platforms.

12. Hyperlinks

12.1 You may not link to any material using or through the Platforms which, if made available through the Platforms, would violate the provisions of this Policy.

13. Harmful software

13.1 The Content may not contain or consist of, and you may not promote, distribute or perform through the Platforms, any viruses, worms, spyware, adware or other harmful or malicious software, programs, routines, applications or technologies.

13.2 The Content may not contain or consist of, and you may not promote, distribute or run through the Platforms, any software, programs, routines, applications or technologies that will or may have a material adverse effect on the performance of a computer or pose material security risks to a computer.

14. Violating the rules

14.1 If you and your users (the stakeholders, such as visitors, exhibitors, speakers, etc.) abide by the above rules, then we will remain best friends. However, if we find that you do not adhere to these rules, we have the right to make the platform unavailable in its entirety (and suspend the agreement-, without entitling you to any damages or refund of amounts already paid. However, you users must also comply with this. If we find that a user does not comply with the rules, you will inform us immediately so that we can take the appropriate (legal) measures.

Chapter 7: General Privacy Policy

Threedee World remains continuously committed to protecting the privacy of its users to the maximum extent possible and strives to provide a safe user experience for everyone. Our Privacy Policy provides everything you need to better understand how Threedee World collects and uses your information, and to understand the choices you have to protect your information.

The Privacy Policy contains our policies regarding the processing of personal data with the explanation of our privacy practices and information. Our privacy policy is designed to inform you about our privacy practices in a clear, concise manner.

If you have a question about privacy you should contact us by emailing us at contact@threedee.world.

The general privacy policy of Threedee World

Capitalized words are defined in the General Terms and Conditions and have the same meaning in this Appendix as in the General Terms and Conditions.

Processing refers to any operation involving personal data that allows a natural person to be identified, directly or indirectly; such as the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, making available, alignment or combination, blocking, erasure or destruction of data.

This Privacy Policy aims to provide the persons involved in those processing operations with all the information required by the regulations in force, including the information required by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation or "GDPR").

Fairtual undertakes to process the Users' personal data in a legal, correct and transparent manner. In this Privacy Statement, Fairtual explains which personal data are processed and what are the purposes in doing so, what rights the User has to secure and possibly improve his/her privacy.

Terms

This Privacy Policy uses the following terms:

The Website: the Website, which can be found at the URL https://threedee.world and all related websites.

The Regulation: the 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 (also referred to as "General Data Protection Regulation" or "GDPR")

Personal data: any information about an identified or identifiable natural person. For example: name, address, family composition, evaluations, testimonials, etc.

Processing: (the set of) processing(s) of personal data. For example: storage, collection, modification, retrieval, consultation, use, transmission, dissemination, transmission, erasure, destruction, etc.

Controller: the natural person, legal person, public authority, department or other body which alone or with others determines the purpose of and means for processing personal data.

Data subject: the identified or identifiable natural person to whom the processed data relates.

To whom does this privacy policy apply?

This policy applies to the processing of personal data of Website Users, specifically:

- persons who visit the Website;
- persons who fill out the contact form.

These individuals will collectively be referred to as the "Data Subjects" and each individually as a "Data Subject".

The controller, data protection officer and processor

- **The Controller**:

  Threedee World BV, whose registered office is located at 1831 Diegem (Belgium), Leonardo da Vincilaan 19A 8, registered with the Crossroads Bank for Enterprises under the number BE0726.840.893 (hereinafter referred to as "Threedee World") is responsible for the processing of personal data that it carries out in the context of its activities;

- **The Data Protection Officer**:

  The data and privacy protection officer at Threedee World can be reached using the following contact information:

  - naam: Mike Thevissen
  - tel: + 32 (0)472 75 66 22
  - E-Mail: dpo@threedee.world

Purpose of processing

Threedee World processes personal data in connection with the use of its Website. Personal data is used for the following purposes:

- Contacts at Users who are enterprises or acting in a professional capacity (customers or prospects): the personal data are necessary to properly prepare and execute the contract concluded with Fairtual. For contract conclusion, Threedee World must have the necessary personal data in order to provide the agreed service;
- Suppliers with whom Threedee World is in contact: the personal data are necessary in order to properly prepare and execute the contract concluded with Fairtual;
- Any legitimate interest of the Controller;
- Being able to fulfill the request of the User who fills out the contact form (consent).

All personal data collected are processed administratively and possibly later for accounting purposes.

What personal data is collected?

Directly collected information

- Information regarding the Data Subject: Name - First Name
- Information to contact the Data Subject: phone number - e-mail address

If the Data Subject makes himself/herself known through the Website (by filling in the contact form), his/her data will be stored in the database. By registering and/or identifying, the Data Subject gives express consent to be included in the database.

What the Data Subject communicates

If the Data Subject contacts Threedee World by telephone, Threedee World may note his/her identity (surname and first name) and telephone number in order to build a contact record and see who uses the service.

Categories of personal data processed

- Identity Information
- Contact information
- All the data, documents and media that the data subject has made available to Threedee World

Who receives the personal data?

The Controller may transfer the Data Subject's personal data to the following recipients:

- ICT service providers;
- Accountant - bookkeeper;
- Subcontractors affiliated with the Controller, such as a designer or programmer.

In principle, the personal data of the Data Subject will not be transferred to a country that is not part of the European Economic Area.

Threedee World processes these personal data in accordance with the purposes specified in the article "Data Processing". Only employees within the Threedee World organization, who in the performance of their duties need this personal data, will be able to consult it.

How long will personal data be kept?

The Controller retains the Personal Data of the Data Subject:

- As long as necessary to achieve the purposes defined in Article Data Processing;
- As long as necessary to delete the personal data after the retention periods provided for in the regulations have expired;
- As long as necessary to comply with obligations arising from a legal text, other regulations or agreements concluded by Threedee World, or imposed by a public authority.

What rights can the data subject exercise?

Right to object

Where personal data are processed on the basis of consent of the Data Subject (see section 'To whom does this policy apply?'), the Data Subject may withdraw this consent at any time.

If the Data Subject wishes to exercise one or more of the rights listed below, he/she should contact the Data Protection Officer of Threedee World using the contact details listed in article 'The Controller and the Data Protection Officer'.

Right to view

The Data Subject has the right to obtain a determination from Threedee World as to whether or not personal data concerning him/her are being processed and, if necessary, to access the personal data in question and the following information:

- the purposes of processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom personal data are disclosed;
- if possible, the period during which the personal data are expected to be
- be stored, or if not possible, the criteria for determining that period;
- that the Data Subject has the right to request Threedee World that personal data be
- erased or corrected, or that the processing be restricted;
- that the Data Subject has the right to complain to the Data Protection Authority;
- all available information about the source of the data, in the event that the
- personal data are not collected from the Data Subject itself;
- the existence, where appropriate, of exclusively automated decision-making, including profiling and, in applicable cases, useful information on the underlying logic, importance and expected consequences of the automated decision-making.

Threedee World will, upon express request of the Data Subject, provide, within a reasonable period of time, the most complete overview of the personal data and/or information requested above. The Data Subject has the right to obtain a copy of the requested information free of charge.

If the Data Subject submits its request electronically, Threedee World may provide the information by electronic means, such as e-mail.

Threedee World guarantees that the Data Subject, through his/her account as a registered User, has full access to his/her data and can change, modify, correct or delete such data himself/herself at any time.

Right of correction

The Data Subject has the right to have erroneous, inappropriate or outdated personal data deleted or corrected. If the Data Subject believes that information stored by Threedee World is incomplete, inaccurate, inappropriate or outdated, he/she should contact Threedee World's Data Protection Officer using the contact details listed in Article 4.

Threedee World guarantees that the Data Subject, through his/her account as a registered User, has full access to his/her data and can change, modify, correct or delete this data himself/herself at any time.

Right to delete data

The Data Subject has the right to obtain the erasure of certain personal data when one of the following applies:

- the personal data are no longer necessary for the purposes under which they were collected or processed;
- the Data Subject withdraws the consent on which the processing is based, and there is no other legal basis for the processing;
- the Data Subject objects to processing pursuant to this policy;
- the personal data have been processed unlawfully;
- the personal data must be deleted in order to comply with a legal obligation incumbent on Threedee World.

Threedee World is obliged to delete personal data without unreasonable delay when one of the above cases applies. Threedee World guarantees that the Data Subject, through his/her account as a registered User, has full access to his/her data and can change, modify, correct or delete such data himself/herself at any time.

Right to restriction of processing

The Data Subject has the right to obtain, in certain cases, the restriction of the processing of his personal data. The following conditions must apply:

- if the personal data stored are inaccurate, for the period Fairtual needs to verify the accuracy of the personal data and, if necessary, to correct it;
- the processing of personal data is unlawful and the Data Subject opposes the erasure of the personal data and requests the restriction of its use;
- Threedee World no longer needs the data for the processing purposes for which the data were stored but in the context of legal proceedings, for the protection of natural or legal persons or for important reasons of public interest.

Where the processing of personal data has been restricted, Threedee World may continue to store the personal data but no personal data may be processed without the prior consent of the Data Subject.

Threedee World guarantees that the Data Subject, through his/her account as a registered User, has full access to his/her data and can modify, adapt, correct or delete such data himself/herself at any time.

Right to transferability of personal data

Subject to the rights and freedoms of third parties and the limitations provided for in the Regulation, the Data Subject has the right to obtain the personal data concerning him that he himself has provided to Threedee World in a structured, common and machine-readable form.

The Data Subject has the right to transfer this data itself to another Controller or to request that the personal data be transferred directly from Threedee World to another Controller.

Refusal of automated processing and decision-making

The data processing operations and processes are neither automated nor without human intervention. Nevertheless, the Data Subject may object to the automated processing of his/her personal data if such processing significantly affects him/her.

The following exception applies here, which must be assessed on a case-by-case basis:

- the automated processing is authorized by a legal provision applicable to Threedee World, which also provides for the necessary measures to protect the rights, freedoms and interests of the Data Subject.

The Data Subject also has the right to object to the processing of personal data applicable to him in the cases provided by law or other regulatory texts.

The Data Subject may exercise these rights by submitting a request to or contacting the Data Protection Officer at Threedee World, as previously mentioned.

The Data Protection Officer will take the necessary measures to verify the identity of the Data Subject making a request.

The Data Subject also has the right to lodge a complaint with the supervisory authority. In Belgium, since May 25, 2018, this is the Data Protection Authority (formerly the Commission for the Protection of Privacy): see https://www.gegevensbeschermingsautoriteit.be.

What security measures are taken?

As personal data is processed, Threedee World guarantees the confidentiality, integrity and availability of this information at all times. Threedee World maintains a high level of security for the processing and the data being processed and stored.

The main principles applied by Threedee World are:

1. Definition of information security roles and responsibilities to ensure that all security activities are carried out.

2. All required documentation, such as policies, standards, procedures and guidelines, is in place to support security. That documentation is reviewed regularly.

3. Threedee World uses a risk-based approach to identify necessary technical and other security controls. This ensures that appropriate priorities are set and that only efficient and effective security controls are selected and implemented.

4. Threedee World is committed to ensuring that employees throughout the organization are aware of the importance of information security and data protection and integrates this through regular training and exercises.

5. Threedee World has identity and access controls in place to protect information from unauthorized access, modification or deletion, whether intentionally caused or not.

6. Threedee World has implemented physical controls to ensure fire and theft prevention and access control for its premises.

7. Cyber protection controls were installed. Applications and technology platforms were designed, configured, maintained and evaluated based on recognized security criteria, such as vulnerabilities and threats are continuously monitored.

8. A Business Continuity program was installed to ensure continuity in case of outages or disasters and restore business processes. During the activation of this program, information security principles remain in effect.

9. Information security policies and their implementation are regularly reviewed.

Chapter 8: Processor Agreement

PARTIES:

You as a customer, hereinafter referred to as "**Controller**";

and

the limited liability company **Threedee World BV**, having its registered office in Belgium, 1831 Diegem, Leonardo da Vincilaan 19A 8, represented in this matter by its director, Mr. Diego Dupont, hereinafter referred to as "**Processor**".

CONSIDERATIONS:

I. Processor has entered into or will enter into one or more agreements with Processor for the provision of various services by Processor to Processor. This agreement or these agreements collectively is or are hereinafter referred to as the "Master Agreement."

II. In performing the Master Contract, Processor shall process data for which Processor is and remains responsible. Such data includes personal data within the meaning of the General Data Protection Regulation (EU 2016/679), hereinafter the "AVG".

III. In view of the provisions of Article 28 paragraph 3 AVG, the parties wish to lay down the conditions of 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 under the Master Agreement involves one or more processing operations listed in **Annex 1**.

1.2 The processing operations of Annex 1 that occur in the provision of the Services are hereinafter referred to as "**the Processes**". The personal data processed thereby: "**the Personal Data**".

1.3 In respect of the Processes, Controller is the Controller and Processor is the Processor. The natural persons who actually use the services of Processor under the Master Contract and, if applicable, their representatives, are also referred to hereinafter as "**the End Users**".

1.4 All terms in this Agreement have the meanings given to them in the AVG.

1.5 The annexes are part of this agreement. They are:

Annex 1	the Processes, the Personal Data and the retention periods;
Annex 2	the Subprocessors and categories of Subprocessors that Controller approves;

Annex 3 Processor's technical and organizational measures;

Annex 4 information regarding a Data Breach.

2 Subject Matter.

2.1 Processor undertakes to process Personal Data solely for the purposes of the activities specified in this Processor Agreement and/or the Master Agreement. Processor guarantees that, without the express and written consent of Controller, it will not use the Personal Data processed under this Processor Agreement in any way for its own purposes or the purposes of third parties, unless a legal provision applicable to Processor obliges it to process. In that case, the Processor shall notify the Controller, prior to the Processing, without delay of that legal requirement, unless that law prohibits such notification for important reasons of public interest.

2.2 Processor shall keep Controllor's Personal Data separate from (Personal) Data it Processes for itself or for third parties.

2.3 Processor shall perform the Processing in a proper and careful manner.

3 Security measures

3.1 Processor takes all technical and organizational security measures required of it under the AVG and in particular under Article 32 AVG.

3.2 Processor will provide a document stating the appropriate technical and organizational measures. This document will be attached to this Processor Agreement as Annex 3.

4 Data breaches

4.1 Processor shall notify Controller without unreasonable delay, but in any case within 24 hours, of any "personal data breach" as referred to in Article 4 sub 12 AVG. Such a breach is hereinafter referred to as "Data Breach".

4.2 Processor shall provide the Controller without unreasonable delay with all information in its possession that is necessary to comply with the obligations under Article 33 AVG and shall provide all cooperation requested by Controller. Processor shall otherwise provide the relevant information as soon as possible in a common format to be determined by Processor. Furthermore, the Processor shall keep the Controller informed of any new developments concerning the Data Breach as well as take all reasonable measures in order to remedy the Data Breach and limit the (possible) consequences thereof as much as possible. Processor will also take those measures necessary to prevent a recurrence of the Data Breach.

4.3 Processor will not notify the Controller about a Data Breach if it is entirely clear that the Data Breach does not pose any risk to the rights and freedoms of natural persons. If there is room for doubt in this respect, the Processor does report the Data Breach to the Controller in order to enable the Controller to form its own opinion regarding a possible report of the Data Breach. Processor shall document all

breaches, including those that do not have to be reported to the Controller, and provide that documentation to the Controller once per quarter or sooner if the Controller requests it. The documentation shall include, at a minimum, the information referred to in Annex 4.

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

5 Engagement of Subprocessors

5.1 Processor is entitled to engage third parties as Subprocessors in the Processing without the prior written consent of the Controller.

5.2 Processor shall ensure that the relevant third party/parties enter into a contract(s) in which they comply with at least the same legal obligations that Processor has.

5.3 Processor shall inform the Controller about the Subprocessors engaged by it. Controller may then object to additions or substitutions regarding Processor's Subprocessors.

5.4 Controller hereby authorizes in each case the engagement of the Sub-processors and/or categories of Sub-processors listed in Annex 2.

6 Confidentiality obligation

6.1 Processor shall keep the Personal Data confidential. Processor shall ensure that the Personal Data will not directly or indirectly become available to third parties. Third parties also include Processor's staff insofar as it is not necessary for them to take cognizance of the Personal Data. This obligation does not apply if this Agreement provides otherwise and/or insofar as a statutory regulation or judgment requires any disclosure.

6.2 Processor shall ensure that persons, not limited to employees, who participate in Processing at Processor are bound by an obligation of confidentiality with respect to Personal Data.

6.3 Processor shall notify Controller of any request for access, disclosure or other form of retrieval and communication of the Personal Data in violation of the obligation of confidentiality contained in this Article.

7 Retention periods and deletion

7.1 Controller is responsible for determining the retention periods with respect to Personal Data. Insofar as Personal Data are under the control of Controller, it shall itself delete them in a timely manner.

7.2 Processor shall delete the Personal Data within thirty days after the end of the Main Contract or, at the discretion of the Controller, transfer the Personal Data to the Controller, unless the Personal Data must be kept longer, such as in the context of (legal) obligations of the Processor, or if the Controller requests the Processor to keep Personal Data longer and the Controller and the Processor agree on the costs and other conditions of such longer retention, the latter without prejudice to the responsibility of the Controller to comply with the statutory retention periods. Any transfer to the Controller shall be at the Controller's expense.

7.3 Processor shall at the request of Controller certify that the erasure referred to in the preceding paragraph has taken place. Controller may, at its own expense, arrange for an audit to verify that this has indeed occurred. Article 10 of this Agreement shall apply to such verification. To the extent necessary, Processor shall notify all Subprocessors involved in the processing of Personal Data of a termination of the Master Agreement and shall instruct them to act as provided herein.

7.4 Unless the parties agree otherwise, Controller shall itself ensure a back up of the Personal Data.

8 Rights of data subjects

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

8.2 Only to the extent that the above paragraph is not possible, Processor shall provide its full and timely cooperation to Controller in order to:

(i) upon the approval of and at the direction of Controller, allow data subjects to access the Personal Data concerning them,
(ii) delete or correct Personal Data,
(iii) demonstrate that Personal Data have been deleted or corrected if they are incorrect (or, in the event Controller does not agree that the Personal Data are incorrect, record the fact that the data subject considers their Personal Data to be incorrect)
(iv) provide the relevant Personal Data to Controller or to a third party designated by Controller in a structured, common and machine-readable form; and
(v) otherwise provide Controller with the opportunity to comply with its obligations under the AVG or other applicable law regarding processing of the Personal Data.

8.3 The costs of and requirements for the cooperation mentioned in the preceding paragraph shall be determined jointly by the parties. In the absence of an agreement to this effect, the costs shall be borne by the Controller.

9 Liability

9.1 Processor shall be liable to Controller for all damages and costs incurred by Controller as a result of a culpable failure by Processor to fulfill its obligations under this Agreement, including but not limited to damages caused by Processor where processing failed to comply with AVG obligations specifically directed to Processor or acted contrary to the legitimate instructions of Controller.

9.2 Processor shall indemnify Controller for all third party claims resulting from an attributable failure of Processor to perform its obligations to Controller under this Agreement.

9.3 Notwithstanding the provisions of this Article 9, the liability provisions of the Master Agreement shall apply in full.

10 Control

10.1 Controller shall have the right to audit compliance with the provisions of this Agreement whenever reasonably appropriate, but in any event once a year, at its own expense, or to have them audited by an independent chartered accountant or chartered computer scientist.

10.2 If such an audit reveals that Processor has not or has not properly complied with this Agreement and/or applicable legal provisions applicable to the Processing of Personal Data, Processor shall bear the costs of the investigation. Also, Processor shall remedy these shortcomings immediately after becoming aware of the observed shortcomings. This is without prejudice to the other rights of Controller.

10.3 Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations in Article 28 AVG. If the third party engaged by the Controller gives an instruction that in the opinion of the Processor violates the AVG then the Processor shall immediately notify the Controller.

10.4 Controller's investigation will always be limited to Processor's systems used for the Processes. Controller shall keep the information found in the audit confidential and use it only to verify Processor's compliance with its obligations under this Agreement and shall delete the information or parts thereof as soon as possible. Controller guarantees that any third parties engaged will also assume these obligations.
Processor itself shall conduct or arrange for periodic security audits and shall provide an annual summary of the outcome of such audit which shall include, at a minimum, an overview of the risks as well as measures to mitigate and remedy them.

11 Processing of Personal Data Outside the European Economic Area

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

12 Other provisions

12.1 Amendments to this Agreement shall be valid only if agreed upon by the parties in writing.

12.2 The parties will adapt this Agreement to amended or supplemented regulations, additional instructions from the relevant authorities and advancing insight into the application of the AVG (for example, through, but not limited to, case law or reports), the introduction of standard provisions and/or other events or insights that require such adaptation.

12.3 This Agreement shall continue as long as the Master Agreement continues. The provisions of this Agreement shall continue in effect to the extent necessary for the consummation of this Agreement and to the extent intended to survive the termination of this Agreement. The latter category of provisions include, but are not limited to, confidentiality and litigation provisions.

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

12.5 This agreement is exclusively governed by Belgian law.

12.6 Parties will submit their disputes relating to this agreement exclusively to the District Court of Brussels.

_____	_____
By:	By:
In the name of: **Threedee World BV**	In the name of:
Date:	Date:
Place:	Place:

Annex 1

Processing of personal data and retention periods

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

This appendix is part of the Processing Agreement and must be initialed 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.]

- ……
- ……
- ……
- ……
- ……
- ……
- ……
- ……
- ……
- ……
- ……
- ……

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

[Description of what is done with the Personal Data (e.g. storage in a file, e-mailing, etc.), what the purpose of the processing is (e.g. marketing, customer acquisition, execution of agreement) and what resources are used (e.g. CRM -software).]

……
……
……
……
……
……
……
……
……

III. The categories of Data Subjects to whom the Personal Data relates

[Description of the categories of Data Subjects, for example website visitors, subscribers, suppliers, children, employees].

……
……

.....
.....
.....
.....
.....
.....

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

[Description of the usage and retention periods that the processor must adhere to]

.....
.....
.....
.....
.....
.....
.....
.....

Annex 2

Subprocessors/categories of Subprocessors

This annex is part of the Processing Agreement and must be initialed by the parties.

This annex contains an overview of the Subprocessors as mentioned in art. 5.4 of this agreement.

Subprocessors:

Name subprocessor	Address	Contact details	Goal subverwerker
Only on demand available	Only on demand available	Only on demand available	Only on demand available

Annex 3

Security measures of Processor

Translation available upon request.

De organisatie volgt de wetgeving en rechtspraak inzake de AVG op regelmatige tijdstippen op.

Hoofdstuk	Onderwerp	Status
Beveiligingsbeleid en organisatie van informatiebeveiliging	Gegevensbescherming: Er werd een DPO aangesteld die verantwoordelijk is voor het coördineren, adviseren, controleren en sensibiliseren van procedures en richtlijnen omtrent gegevensbescherming. Deze verantwoordelijke zal periodiek worden bijgeschoold zodat zijn kennis en deskundigheid steeds actueel blijft.	Er is een DPO aangeduid die beschikt over de nodige competenties om zijn opdracht uit te voeren. De DPO heeft een duidelijke functieomschrijving en er kunnen geen belangenconflicten ontstaan door andere taken die de DPO uitvoert binnen de organisatie. Er zijn voldoende middelen voorhanden en er wordt voldoende tijd gespendeerd aan de organisatie van informatieveiligheid met betrekking tot de verwerking van persoonsgegevens. Er bestaat een actief beslissingsplatform (DPO + projectteam) dat op regelmatige basis vergadert en beslissingen neemt. Er bestaat eveneens een duidelijke ondersteuning van de directie om de implementatie van de gegevensbescherming in de organisatie op te starten, te beheersen, te onderhouden en waar nodig bij te sturen.
	Beveiligingsverantwoordelijkheden: Er zijn formele beleidsteksten omtrent gegevensbescherming goedgekeurd en bekend onder de medewerkers. De verantwoordelijkheden omtrent gegevensbescherming zijn intern toebedeeld.	Er bestaat een algemeen informatieveiligheidsbeleid met betrekking tot de verwerking van persoonsgegevens, die zowel intern als extern werd / wordt gecommuniceerd en dat regelmatig wordt geëvalueerd. Er bestaat een actieve ondersteuning vanuit de directie naar de freelancers met wie wordt samengewerkt met betrekking tot de naleving van het algemeen informatieveiligheidsbeleid met betrekking tot de verwerking van persoonsgegevens.
	Risicobeheer: Er werd een formele risicoanalyse uitgevoerd waaruit maatregelen ten aanzien van gegevensbescherming werden opgesteld. Dit proces zal periodiek worden herhaald.	Er werd en er wordt op regelmatige basis een risicoanalyse uitgevoerd om te beoordelen wat de risico zijn bij verlies, onrechtmatige overdracht, wijziging… van persoonsgegevens. Er werd en wordt op regelmatige basis een afweging gemaakt tussen de kostprijs voor het nemen van technische en organisatorische maatregelen t.o.v. de risico's van eventuele inbreuken en de gevolgen ervan voor de rechten en vrijheden van betrokkenen. Er werden en worden regelmatig technische en organisatorische maatregelen genomen om risico's te vermijden die een invloed kunnen hebben op de rechten en vrijheden van betrokkenen.
Veilig personeelsbeleid	Vertrouwelijkheidsverplichtingen: De medewerkers zijn onderworpen aan een vertrouwelijkheidsverplichting bij het verwerken van persoonsgegevens. Deze verplichting is opgenomen in de arbeidsovereenkomst of in het arbeidsreglement.	De Verwerker heeft geen personeel in dienst. Met alle freelancers werd een vertrouwelijkheidsovereenkomst afgesloten. Er bestaan interne disciplinaire maatregelen voor overtredingen die betrekking hebben op de omgang met persoonsgegevens. Er wordt op regelmatige basis gecontroleerd op welke manier medewerkers met persoonsgegevens omgaan.
	Sensibilisering: De medewerkers zijn zich bewust van het belang van gegevensbescherming en zullen de nodige procedures volgen bij de verwerking van persoonsgegevens. Deze sensibilisering zal periodiek worden herhaald	Elke freelancer die met de Verwerker samenwerkt heeft diverse awareness-trainingen gevolgd zowel op het gebied van GDPR als op het gebied van cyber security.
	In- en uitdiensttreding: De toegangsrechten van de verschillende werknemers worden bij de beëindiging van de samenwerking stopgezet zodat onbevoegden geen toegang meer hebben tot de persoonsgegevens.	Er wordt rekening gehouden bij interne verschuivingen van medewerkers die persoonsgegevens verwerken of zullen verwerken. Toegangsrechten en andere rechten worden desgevallend geëvalueerd en aangepast.
Inventaris van bedrijfsmiddelen	Inventaris van bedrijfsmiddelen: Er wordt een inventaris bijgehouden van alle informatie verwerkende systemen die worden gebruikt door de werknemers.	Er wordt op organisatieniveau een duidelijk onderscheid gemaakt tussen persoonsgegevens, anonieme gegevens, gecodeerde gegevens en gevoelige gegevens.

Cryptografie	Bedrijfsmiddelen: Alle informatie verwerkende systemen waarop informatie van de verwerkingsverantwoordelijke worden verwerkt zijn passend geëncrypteerd.	Er bestaat een beleid omtrent gebruik van encryptie dat wordt afgestemd met de risicoanalyse om de vertrouwelijkheid, authenticiteit en/of integriteit van persoonsgegevens te beschermen. De organisatie heeft een beleid ontwikkeld voor de bescherming van de levensduur van cryptografische sleutels tijdens hun gehele levenscyclus.
	Informatietransfers: Alle vertrouwelijke gegevens van de verwerkingsverantwoordelijke worden enkel getransfereerd met behulp van een beveiligde verbinding.	Er wordt steeds gebruik gemaakt van beveiligde verbindingen.
Fysieke beveiliging	Fysieke toegang: Toegang tot de gebouwen waar persoonsgegevens worden verwerkt is enkel toegankelijk voor geïdentificeerde en geautoriseerde personen.	Er worden gepaste beveiligingsmaatregelen genomen inzake fysieke beveiliging van lokalen en gebouwen. Er wordt rekening gehouden met elke potentiële vorm van schade (brand, water…). Er wordt rekening gehouden met de beveiliging van apparatuur, bekabeling en de ondersteunende voorzieningen om verlies, schade, diefstal en het ongewenst veranderen van persoonsgegevens te voorkomen. Er wordt bijzondere aandacht besteed aan apparatuur die zich buiten het terrein van de organisatie bevindt of wordt gebruikt.
Toegangscontrole	Toegangsbeleid: De rechten van iedere werknemer zullen beperkt worden volgens het 'need-to-know' principe. Meer toegang dan initieel noodzakelijk zal enkel mogelijk zijn naar een formele goedkeuring en bij de aanwezigheid van een geldige reden.	Er bestaat een actueel en gedocumenteerd toegangsbeleid waarbij duidelijk is wie toegang heeft tot welke persoonsgegevens. Hier wordt rekening gehouden met Dataclassificatie. Er is een verantwoordelijke aangesteld voor de aanvragen met betrekking tot de toegangsrechten. Deze verantwoordelijke is verschillend van de persoon die de toegangsrechten op technisch niveau in de systemen toekent, aanpast of verwijdert. Er bestaan passende beveiligingsmaatregelen omtrent toegang tot data (zoals paswoordbeveiliging). Er bestaat functiescheiding om te verhinderen dat één persoon alle rechten heeft.
	Toegangsautorisatie: Om toegang te krijgen tot gevoelige informatie is er een passend autorisatiesysteem. Ieder individu zal een unieke ID krijgen waarmee hij kan inloggen.	
	Authenticatie: Voor de authenticatie van gebruikers is er een sterk authenticatiesysteem geïmplementeerd. Indien toegang tot gevoelige persoonsgegevens via internet mogelijk is moet er gebruik worden gemaakt van multi-factor authenticatie.	
	Netwerktoegang: Er is een systeem aanwezig die een redelijke mate van zekerheid biedt dat toegang tot het netwerk gepast wordt beschermd (bv. firewalls, securityvoorzieningen,…)	Netwerkbeveiliging (firewall, WiFi…) maakt onderdeel uit van het informatieveiligheidsplan.
Operationele beveiliging	Back-up: Er worden op periodieke basis back-ups genomen van de persoonsgegevens. Deze back-ups zullen geëncrypteerd worden bewaard op een externe locatie.	Er bestaat een geschikt back-up beleid, welke regelmatig wordt getest en opgevolgd om een adequaat herstel te waarborgen na schade, verlies, diefstal en ongewenste wijziging van persoonsgegevens. Er bestaat een beleid omtrent gebruik van encryptie dat wordt afgestemd met de risicoanalyse om de vertrouwelijkheid, authenticiteit en/of integriteit van persoonsgegevens te beschermen. De organisatie heeft een beleid ontwikkeld voor de bescherming van de levensduur van cryptografische sleutels tijdens hun gehele levenscyclus.
	Beveiligingsupdates: Beveiligingsupdates en -patches worden systematisch opgevolgd en geïnstalleerd.	Er bestaat geüpdatete bescherming tegen malware. Er heerst voldoende bewustzijn bij de systeem- en de eindgebruikers. Beveiligingsupdates worden regelmatig uitgevoerd.
Communicatie-beveiliging	Transfer over netwerken: Alle persoonsgegevens die worden verzonden via publieke of interne kanalen of netwerken zullen adequaat worden versleuteld.	Er bestaat een e-mail- en internetbeleid (transport), waarbij men bijzondere aandacht besteedt aan het gebruik van persoonsgegevens in e-mail.
Leveranciers-relaties	Keuze van Subverwerkers/onderaannemers: Er wordt een adequaat selectieproces gehanteerd bij de keuze van Subverwerkers/onderaannemers waarbij de beveiliging van persoonsgegevens wordt geëvalueerd. Enkel partijen die voldoen aan de huidige standaarden op vlak van informatieveiligheid en	De beveiligingsinspanningen van de informatiesystemen van de subverwerkers / onderaannemers worden bij aanschaf gecontroleerd. Ook bij de ontwikkeling van nieuwe informatiesystemen of bij uitbreidingen van bestaande informatiesystemen (toepassingen, diensten, IT-middelen of andere informatie verwerkende onderdelen…) wordt er controle uitgeoefend op de beveiligingseisen.

	gegevensbescherming zullen worden gebruikt voor de verwerking van persoonsgegevens.	
	Contractuele verplichtingen: Er is een verwerkersovereenkomst aanwezig met alle mogelijke leveranciers die persoonsgegevens zullen verwerken. Deze overeenkomst bevat alle verplichte bepalingen en werd ondertekend.	Er zijn juridisch goedgekeurde verwerkersovereenkomsten voorhanden met externe verwerkers. Verwerkersovereenkomsten worden gecheckt op beveiliging van persoonsgegevens. De verwerkersovereenkomsten bevatten voldoende garanties dat de (sub)verwerker(s) persoonsgegevens verwerken dit doen conform de AVG. Er wordt controle uitgeoefend op deze (sub)verwerker(s) teneinde de conformiteit aan de AVG te waarborgen.
Beheer van informatie-beveiligings-incidenten	Incident management: Er is een interne procedure die garandeert dat mogelijke beveiligingsinbreuken ook worden gemeld en vervolgens worden afgehandeld door de verantwoordelijken. Deze procedure werd ook duidelijk intern gecommuniceerd. Alle mogelijke beveiligingsinbreuken worden op een centrale plaats verzamelt.	Er wordt voor gezorgd dat aan de hand van gedocumenteerde procedures kan gedetecteerd, gehandeld en gerapporteerd worden inzake incidenten. Bij incidenten wordt de DPO onmiddellijk op de hoogte gebracht. De DPO kent alle zwakke plekken die kunnen leiden tot incidenten, alsook de oplossingen die risico's kunnen vermijden. Bij een voorkomend incident liggen de verantwoordelijkheden vast.
	Notificatie van incidenten: Bij een mogelijk beveiligingsincident dat een impact heeft op de vertrouwelijkheid, integriteit of beschikbaarheid van persoonsgegevens zullen de nodige stappen worden ondernomen om de verwerkingsverantwoordelijke tijdig en voldoende in te lichten hierover.	De organisatie is in staat de continuïteit en de beschikbaarheid van de persoonsgegevens steeds te waarborgen op basis van de resultaten van een risicoanalyse. Er bestaat een bedrijfscontinuïteitsplan. De organisatie voorziet voldoende redundantie (= het voorkomen van iets) binnen de gegevensverwerkende diensten om de beschikbaarheid van persoonsgegevens te waarborgen. Bijkomende gegevensbeschermingsrisico's als gevolg van redundantie worden hierbij in acht genomen.
Bedrijfscontinuïteit	Noodherstel: Er is een gepast systeem aanwezig om in geval van storingen de beschikbaarheid en integriteit van gegevens te garanderen	Er bestaat een privacyverklaring die voldoet aan AVG en volgende gegevens bevat: • De identiteit van de verwerkingsverantwoordelijke • De doeleinden waarvoor de gegevens zullen worden verwerkt • De persoonsgegevens die per doeleinde worden verwerkt • De wettelijke grondslag voor gegevensverwerking • De bewaartermijnen • Of de gegevens uitgewisseld worden buiten de Europese Unie • De mogelijkheid voor de betrokkene om een klacht in te dienen bij de GBA indien hij/zij meent dat zijn/haar persoonsgegevens foutief worden verwerkt • De rechten voor de betrokkenen • De technische en organisatorische maatregelen die de organisatie neemt ter bescherming van de persoonsgegevens Er bestaat een register van verwerkingsactiviteiten dat voldoet aan de AVG wetgeving. Dit register bevat: • de naam en contactgegevens van de (gezamenlijke) verwerkingsverantwoordelijke, van de vertegenwoordiger van de verwerkingsverantwoordelijke en/of van de functionaris voor gegevensbescherming • de verwerkingsdoeleinden • een beschrijving van de categorieën van betrokkenen • een beschrijving van de categorieën van persoonsgegevens? • de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt • de ontvangers in derde landen of internationale organisaties • de bewaartermijnen • een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen? • doorgiften van persoonsgegevens aan een derde land of een internationale organisatie en indien nodig de documenten inzake de passende waarborgen? Er kan voldaan worden aan verzoeken van betrokkenen met betrekking tot hun rechten: • De rechten van betrokkenen worden in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ter beschikking gesteld van betrokkenen? • De organisatie komt tegemoet aan het recht op informatie. • De organisatie komt tegemoet aan het recht van inzage. • De organisatie komt tegemoet aan het recht op correctie. • De organisatie komt tegemoet aan het recht op verwijdering / recht op vergetelheid.

Annex 4

Information regarding a Data Breach.

The Processor will provide all information that the Controller deems necessary to assess the Data Breach or incident. In any case, the Processor provides the following information to the Controller:

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