GoalGorilla

Data Processing Agreement

Date:

January 2018

Version:

1.1

This data processing agreement is an appendix to “Offer” (hereinafter: the Agreement) by and between Customer (hereinafter: Controller) and GoalGorilla (hereinafter: Processor).

Article 1. Purposes of processing

1.1. Processor hereby agrees under the terms of this Data Processing Agreement to process personal data on behalf of the Controller. Processing shall be done solely for the purpose of the Agreement, in particular for storing data in the ‘cloud’ for the benefit of Controller, and associated online services, and all purposes compatible therewith or as determined jointly.

1.2. The personal data to be processed by Processor for the purposes as set out in the previous clause and the categories of data subjects involved are set out in Appendix 1 to this Data Processing Agreement. Processor shall not process the personal data for any other purpose unless with Controller’s consent. Controller shall inform Processor of any processing purposes to the extent not already mentioned in this Data Processing Agreement. Processor however is permitted to use personal data for quality assurance purposes, including surveys to data subjects and statistical research purposes regarding the quality of Processor’s services.

1.3. All personal data processed on behalf of Controller shall remain the property of Controller and/or the data subjects in question.

Article 2. Processor obligations

2.1. Regarding the processing operations referred to in the previous clause, Processor shall comply with all applicable legislation, including at least all data processing legislation such as the Dutch Data Protection Act.

2.2. Upon first request Processor shall inform Controller about any measures taken to comply with its obligations under this Data Processing Agreement.

2.3. All obligations for Processor under this Data Processing Agreement shall apply equally to any persons processing personal data under the supervision of Processor, including but not limited to employees in the broadest sense of the term.

2.4. Processor shall inform Controller without delay if in its opinion an instruction of Controller would violate the legislation referred to in the first clause of this article.

2.5. Processor shall provide reasonable assistance to Controller in the context of any privacy impact assessments to be made by Controller.

Article 3. Transfer of personal data

3.1. Processor may process the personal data in any country within the European Union.

3.2. In addition Processor may transfer the personal data to a country outside the European Union, provided that country ensures an adequate level of protection of personal data and complies with other obligations imposed on it under this Data Processing Agreement and the Dutch Data Protection Act, including the availability of appropriate safeguards and enforceable data subject rights and effective legal remedies for data subjects.

3.3. Processor shall report to Controller of the countries involved. Processor warrants that, considering the circumstances that apply to the transfer of personal data or any category of

transfers, the country or countries outside the European Union have an adequate level of protection.

3.4. In particular Processor shall take into account the duration of the processing, the country of origin and the country of destination, the general and sector-based rules of law in the country of destination and the professional rules and security measures which are complied with in that country.

Article 4. Allocation of responsibilities

4.1. Processor shall make available IT facilities to be used by Controller for the purposes mentioned above. Processor shall not itself perform processing operations unless separately agreed otherwise.

4.2. Processor is solely responsible for the processing of personal data under this Data Processing Agreement in accordance with the instructions of Controller and under the explicit supervision of Controller. For any other processing of personal data, including but not limited to any collection of personal data by Controller, processing for purposes not reported to Processor, processing by third parties and/or for other purposes, the Processor does not accept any responsibility.

4.3. Controller represents and warrants that the content, usage and instructions to process the personal data as meant in this Data Processing Agreement are lawful and do not violate any right of any third party.

Article 5. Involvement of sub-processors

5.1. Processor shall involve third parties in the processing under this Data Processing Agreement on the condition that such parties are reported in advance to the Controller; Controller may object to a specific third party if its involvement would reasonably be unacceptable to it.

5.2. In any event, Processor shall ensure that any third parties are bound to at least the same obligations as agreed between Controller and Processor. Controller has the right to inspect the agreements containing such obligations.

5.3. Processor represents and warrants that these third parties shall comply with the obligations under this Data Processing Agreement and is liable for any damages caused by violations by these third parties as if it committed the violation itself.

Article 6. Security

6.1. Processor shall use reasonable efforts to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk for the processing operations involved, against loss or unlawful processing (in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed).

6.2. Processor shall implement at least the specific security measures included in the Security Protocol available under the name “Critical Security Controls (CSC) of CIS”. Processor may adjust the Security Protocol at any time unilaterally. Processor shall inform Controller of any

adjustments.

6.3. Processor does not warrant that the security is effective under all circumstances. If any security measure explicitly agreed in this Data Processing Agreement is missing, then Processor shall use best efforts to ensure a level of security appropriate to the risk taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

6.4. Controller shall only provide personal data to Processor for processing if it has ensured that the required security measures have been taken. Controller is responsible for the parties' compliance with these security measures.

6.5. Processor has available a Third Party Memorandum (TPM) regarding the security measures for personal data implemented by it. This TPM will be made available to Controller upon request.

Article 7. Notification and communication of data breaches

7.1. Controller is responsible at all times for notification of any security breaches and/or personal data breaches (which are understood as: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed) to the competent supervisory authority, and for communication of the same to data subjects. In order to enable Controller to comply with this legal requirement, Processor shall notify Controller within 48 hours after becoming aware of an actual or threatened security or personal data breach.

7.2. A notification under the previous clause shall be made at all times, but only for actual breaches.

7.3. The notification shall include at least the fact that a breach has occurred. In addition, the notification shall:

- describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Article 8. Processing requests from data subjects

8.1. In the event a data subject makes a request to exercise his or her legal rights under data protection legislation to Controller, Processor shall pass on such request to Controller, and Controller shall process the request. Processor may inform the data subject of this passing on.

Article 9. Confidentiality obligations

9.1. All personal data that Processor receives from Controller and/or collects itself is subject to strict obligations of confidentiality towards third parties. Processor shall not use this information for any goals other than for which it was obtained, not even if the information has been converted into a form that is no longer related to an identified or identifiable natural person.

9.2. The confidentiality obligation shall not apply to the extent Controller has granted explicit permission to provide the information to third parties, the provision to third parties is reasonably necessary considering the nature of the assignment to Controller or the provision is legally required.

Article 10. Audit

10.1. Controller has the right to have audits performed on Processor by an independent third party bound by confidentiality obligations to verify compliance with the security requirements, compliance with data processing regulations, unauthorised use of personal data by Processor personnel, compliance with the Data Processing Agreement, and all issues reasonably connected thereto.

10.2. This audit may be performed once every quarter as well as in the event of a substantiated allegation of misuse of personal data .

10.3. Processor shall give its full cooperation to the audit and shall make available employees and all reasonably relevant information, including supporting data such as system logs.

10.4. The audit findings shall be assessed by the parties in joint consultation and may or may not be implemented by either party or jointly.

10.5. The costs of the audit shall be borne by Controller.

Article 11. Liability and contractual fine

11.1. The liability of parties for any damages as a result of a reputable failure to comply with this Data Processing Agreement, unlawful acts or otherwise, is excluded. To the extent such liability cannot be excluded, it is limited to direct damages per event (a sequence of successive events counting as one event), up to the amount received by the other Party for all activities under this Data Processing Agreement for the month prior to the event. Any liability of the parties for direct damages shall in any event never be more than € 1.000.000.

11.2. Direct damages shall include only:

- damages to physical objects;
- reasonable and proven costs to cause the party in question to regain compliance with this Data Processing Agreement;
- reasonable costs to assess the cause and extent of the direct damage as meant in this article; and
- reasonable and proven costs that Controller has incurred to limit the direct damages as meant in this article.

11.3. Any liability for indirect damages by the Parties for indirect damages is excluded. Indirect

damages are all damages that are not direct damages, and thus including but not limited to consequential damages, lost profits, missed savings, reductions in goodwill, standstill damages, failure to meet marketing requirements, damages as a result of using data prescribed by Controller, or loss, corruption or destruction of data.

11.4. No limitation of liability shall exist if and to the extent the damages are a result of intentional misconduct or gross negligence on the part of the party in question or its directors.

11.5. Unless a failure by the party in question is incapable of redress, any liability shall exist only if the other party puts the responsible party on notice of default, including a reasonable term for addressing the failure, and the responsible party fails to comply even after this term. The notice shall contain a detailed description of the failure to ensure that the responsible party has a reasonable opportunity to address the failure.

11.6. Any claim for damages either party to the other that is not specifically notified in detail shall be extinguished by the passage of twelve (12) months after the date its cause first arose.11.7. The parties shall maintain adequate professional liability insurance for any liability under this article. The insurance policy shall be made available upon request.

Article 12. Term and termination

12.1. This Data Processing Agreement enters into force upon signature by the parties and on the date of the last signature.

12.2. This Data Processing Agreement is entered into for the duration of the Agreement.

12.3. Upon termination of the Data Processing Agreement, regardless of reason or manner, Processor shall - at the choice of Controller - return in original format or destroy all personal data available to it.

12.4. This Data Processing Agreement may be changed in the same manner as the Agreement.

Appendix 1: Stipulation of personal data and data subjects

Personal data

Processor shall process the below personal data under the supervision of Controller, as specified in article 1 of the Data Processing Agreement:

- Names and addresses
- Telephone numbers
- Email addresses
- Visitor behaviour
- IP addresses
- Social media accounts
- (Portrait) photos
- Dates of birth

Of the following categories of data subjects:

- Account holders
- Website visitors

Controller represents and warrants that the description of personal data and categories of data subjects in this Appendix 1 is complete and accurate, and shall indemnify and hold harmless Process for all faults and claims that may arise from a violation of this representation and warranty.