PROCESSOR AGREEMENT FULL SERVICE HOSTING

Definitions

This Processor Agreement applies to all forms of Personal Data Processing that Full Service Hosting, hereinafter referred to as "Full Service Hosting", established in Utrecht, registered with the Chamber of Commerce under number 70645965, (hereinafter: Processor) executes for the benefit of another party to whom it provides services (hereinafter: Controller).

Hereinafter referred to collectively as “Parties”;

Taking into consideration that:

• Parties have entered into an agreement with regard to hosting services and domain name registrations,hereinafter referred to as "Agreement". For the execution of the Agreement, Processor will process Personal Data for the benefit of the Controller;

• Parties wish to treat the Personal Data that will be processed for the performance of the Agreement with care and according to the GDPR and other applicable laws and regulations regarding the Processing of Personal Data.

• In accordance with the GDPR and other applicable laws and regulations concerning the Processing of Personal Data, the Parties wish to record their rights and obligations with respect to the Processing of Personal Data of the Concerned in writing in this Processor Agreement.

• Only the Controller determines the purpose of and the means for the Processing of Personal Data. The Processor has no influence on this;

Have agreed as follows:

1. Concepts

1.1. Concerned: person to whom Personal Data relates.

1.2. Data Breach: a security breach of Personal Data that has serious adverse consequences for the protection of Personal Data.

1.3. Employees: the persons engaged by the Parties for the implementation of this Processor Agreement, who will work under their responsibility.

1.4. Personal Data: any information regarding an identified or identifiable natural person. Pseudonymized Personal Data (traceable) are also included.

1.5. Sub processor: a third party that is engaged by the Processor to process Personal Data, without being subject to the direct authority of the Processor.

1.6. Controller: responsible for the Processing within the meaning of the Dutch Personal Data Protection Act (Wbp) and/or European regulations and directives with regard to the protection of Personal Data (GDPR).

1.7. Processor: the person who processes Personal Data for the benefit of the Controller without being subject to his direct authority.

1.8. Processing: any act or acts relating to Personal Data, including collecting, recording, organizing, storing, updating, amending, retrieving, consulting, using, providing by means of forwarding, distributing or any other form of posting, linking together, as well as the protection, erasing, or destruction of data.

2. Subject

2.1. If the Processor has access to the Personal Data only, without an obligation to process these, the Processor will observe both the national and international laws and regulations relating to Personal Data and the provisions of this Processor Agreement, if and insofar the Controller has emphasized the presence of Personal Data and the place (path) where these Personal Data are located.

2.2. If the Processor has committed to the Processing of Personal Data in the Agreement, Processor will do this with great care and in accordance with the purposes of the Processing. Processor will also observe the national and international laws and regulations regarding Personal Data and the provisions of this Processor Agreement, if and insofar the Controller has emphasized the presence of Personal Data and the place where these Personal Data are located.

3. Obligations of the Controller

3.1. The Controller will inform Processor about any changes regarding the Processing (if applicable) and any consequences in a timely matter, in general within 10 working days.

3.2. Controller guarantees that the assignment for the Processing of Personal Data (if applicable) is not unlawfuland does not infringe the rights of third parties.

4. Obligations of the Processor

4.1. Processor will only view and/or process the Personal Data if and insofar this is necessary for the implementation of the Agreement and will follow all reasonable instructions of the Controller.

4.2. Processor will not store the Personal Data at a location outside the European Economic Area. For domain registrations, it may be necessary to pass on Personal Data to countries outside the European Economic Area. This is then limited to what is required by the relevant registry.

4.3. Processor warrants that its Employees shall comply with the provisions of this Processor Agreement, if and insofar as they are involved in the Processing of Personal Data in any way. The Employees of the Processor are bound by an obligation of secrecy.

4.4. Processor has appointed a data protection officer.

4.5. At the first request of the Controller, Processor will immediately hand over or destroy all copies of Processed Personal Data, originating from or processed on the behalf of the Controller.

4.6. Processor will take appropriate technical and organizational security measures to protect the Personal Data against loss and unlawful Processing. Taking into account the state of technology and the costs of its implementation, these measures guarantee an appropriate level of security in view of the risks involved in the Processing and the nature of the data to be protected.

4.7. Processor maintains a register of all categories of Processing activities that he has carried out for the Controller.

4.8. Processor shall provide Controller with full and timely cooperation to allow the Concerned to inspect their Personal Data, to have their Personal Data deleted or corrected, and/or to show that these Personal Data have been removed or amended. If the Controller disputes the position of the Concerned, he needs to record that the Concerned regards his Personal Data as incorrect.

4.9. The Processor takes adequate internal management measures to fulfill the obligations arising from this Agreement and records them in a way that makes it easy to monitor compliance. With the Processing of Personal Data, activities and incidents relating to the Personal Data are recorded in log files.

4.10. At the Controllers' instructions, the Processor will cooperate with encryption and pseudonymization of Personal Data. If this results in higher costs for the Processor, the Controller will reimburse these costs.

4.11. Once a year, the Controller may have the Processing of Personal Data checked for correct compliance with the Processor Agreement by means of an investigation by an independent register EDP-Auditor. The Auditor has an obligation of secrecy. The Auditor will report to the Controller in general terms, but will not disclose any details of the security measures taken. The costs of the investigation will be charged to the Controller.

4.12. The content and scope of the assignment for Processing and the fee to be paid is in accordance with what has been agreed to in the Agreement. Processor will follow instructions of the Controller regarding the Processing and/or storage of Personal Data.

5. Sub processor

5.1. The Processor can outsource the implementation of the Processor Agreement wholly or partly to a Sub processor. At all times, the Processor remains the point of contact for the Controller and remains responsible for compliance with the provisions of this Processor Agreement.

5.2. The Processor will impose the same obligations on the Sub processor as arising from this Processor Agreement for itself. The Processor will record this in writing in a contract and supervise compliance by the Sub processor. The Processor takes full responsibility towards the Controller for the consequences of outsourcing work to a Sub processor.

5.3. The outsourcing of domain name registrations is an exception to articles 5.1 and 5.2. Depending on the Top-Level Domain, Personal Data may be made public and/or the Processor cannot guarantee the security of Personal Data.

6. Transmission of Personal Data

6.1. The Processor is not permitted to provide Personal Data to Parties other than the Controller, except for a legal obligation or for the Agreement with the Controller.

6.2. If the Processor has to provide Personal Data for a legal obligation, the Processor will:

- verify the basis of the request and the identity of the requester and inform the Controller of this matter before the provision;

- limit the provision to what is legally required;
- enable the Controller to exercise the rights of the Controller and Concerned and defend the
- interests of Controller and Concerned;
- provide the data to the Concerned in a structured, common, and machine-readable form.

7. Security

7.1. Controller and Processor take appropriate technical and organizational measures to ensure a risk-adapted level of security, so that the Processing complies with the requirements of the GDPR and other applicable laws and regulations regarding the Processing of Personal Data, and the protection of the rights of the Concerned are guaranteed. The security measures taken by Processor are included in Appendix A.

7.2. Controller and Processor strive to secure Personal Data and keep it safe from intruders and from external calamities as well as against careless Processing, unauthorized provision or unauthorized disclosure and loss, destruction or damage. Both Parties ensure that their IT facilities and equipment are physically protected from unauthorized access and against damage and malfunctions. They take measures to prevent unauthorized access to information systems.

7.3. Controller and Processor will continuously monitor whether the Processing systems continue to meet adequate requirements of confidentiality, integrity, availability, and resilience (quick recovery after temporary unavailability).

7.4. If the Controller submits a written request, the Processor will take extraordinary measures with regards to the designated (categories of) Personal Data for the security and/or confidentiality. If this results in higher costs for the Processor, the Controller will reimburse these costs.

8. Data Breach

8.1. If the Processor is dealing with a Data Breach, the Processor will report this immediately to the Controller, but in any case, within 24 hours. The Processor will state the nature of the Data Breach, the (alleged) consequences of the breach, and the measures taken to remedy or limit the impacts.

9. Confidentiality

9.1. All information from the Controller and its customers are confidential and will be treated as such by the Processor. The Processor is obliged to confidentiality of all Personal Data, and the processed information or of which Processor becomes aware in the context of the Agreement or this Processor Agreement.

9.2. The confidentiality does not apply to information:

Which is publicly known without this disclosure being the result of an unlawful act;

- Of which release is required as a result of any legal provision or court order, on the condition of prior written notification of the revealing Party to the Party whose information it concerns;
- That has been independently developed by a Party;
- That has been in possession already by a Party without any obligation of confidentiality.
- After the termination of this Processor Agreement, this article and the confidentiality obligation set

- herein will remain in effect.

10. Intellectual property

10.1. The Controller (or a Customer of the Controller) holds all intellectual property rights, including copyright, database rights, and all other intellectual property rights as well as similar rights to the protection of information such as the collection of data and Personal Data, copies or edits thereof.

10.2. The Processor holds all intellectual property rights, including copyright, database rights, and all other intellectual property rights as well as similar rights to the protection of information on the products and services of Processor.

11. Liability and insurance

11.1. The Processor is not liable for damage and fines that are incurred by the Controller as a result of Processors' failure to comply, or breach of the regulations under or pursuant to the Dutch Personal Data Protection Act and/or European regulations and directives regarding the protection of Personal Data and/or other laws and regulations in this area and/or this Processor Agreement.

11.2. If liability has been established by competent authority, the liability of the Processor for damage suffered by the Controller and/or forfeited fines as referred to in Article 11.1 is limited to €1000 per event.

11.3. Controller safeguards Processor from claims from third parties (in particular Concerned) and any damage as a result thereof, based on failure to comply with regulations under or pursuant to the Personal Data Protection Act and/or European regulations and directives with regard to the protection of Personal Data and/or other laws and regulations in this area and/or this Processor Agreement.

12. Duration and termination

12.1. The Processor Agreement shall take effect when the general terms and conditions are accepted.

12.2. The provisions on duration and termination of the Agreement shall be deemed to be provisions on the duration and termination of the Processor Agreement. When for whatever reason the Agreement ends, the Processor Agreement ends as well.

12.3. In the event of termination of the Processor Agreement, the Processor will transfer all Personal Data to the Controller or destroy all the Personal Data in possession of the Processor at the explicit written request of the Controller.

12.4. Obligations that, due to their nature, are intended to continue after the termination of the Processor Agreement, continue to be applicable after termination. These obligations include the provisions concerning confidentiality, transfer and disposal, liability and applicable law.

13. Dissolution

13.1. Each Party may dissolve the Agreement wholly or partially if the other Party fails attributable in the fulfillment of the Processor Agreement and when the shortcoming has not been remedied after a default notice, notwithstanding the right to compensation.

13.2. Either Party may terminate all or part of this Agreement, with immediate effect, if the other Party is granted a suspension of payment if bankruptcy is requested for the other Party, if the company of the other Party is liquidated or terminated other than for reconstruction or merging of companies.

14. Other

14.1. Modifications to this Agreement or additions shall be agreed on in writing between the Processor and the Controller. Changes or additions are recorded in an addendum to this Agreement and are binding if both Parties have signed this addendum.

14.2. When an attempt to resolve any disputes in mutual consultation has been rendered ineffective, any conflicts resulting from this Agreement will be settled by arbitration under the rules and procedures of the Dutch Arbitration Institute, where the arbitrator(s) will apply Dutch law.

Appendix A - Security measures

The minimum measures met by Processor:

1. The Processor upholds a policy paper that explicitly addresses the measures taken by the Processor to protect the Processing of the data, as well as to guarantee privacy.

2. The Employees of the Processor that are involved with Processing Personal Data are bound to an obligation of confidentiality or an integrity code. If applicable, a screening took place prior to the employment.

3. All Employees of the company and (if applicable) hired staff and external users, receive suitable and regular training on the information security policies and the information security procedures of the organization, as far as relevant for their function. During the training, explicit attention is devoted to the handling of Personal Data.

4. IT facilities and equipment are physically protected against unauthorized access, damage, and malfunctions.

5. Procedures are in place to allow authorized users to access the information systems and services they need for the performance of their duties and to prevent unauthorized access to information systems.

6. Adequate encryption must always be applied when transporting confidential information, explicitly designated as such by the Controller, over networks.

7. An up-to-date key plan is applicable for the management of certificates and the associated keys, in which powers and segregation of duties are guaranteed.

8. Procedures are in place for the acquisition, development, maintenance, and destruction of data and information systems.

9. The activities performed by users (regarding Personal Data) are recorded in log files. The same applies to other relevant events, such as attempts to gain unauthorized access to Personal Data and

disruptions that may lead to destruction or loss of Personal Data. Custom logging of specific data is possible through a quote.

10. Security measures are built into all application systems, including adequate access control.

11. The network and the information systems are actively monitored and managed. There's also a procedure to handle any Data Breaches. Informing the Controller is a part of this.

12. The Processor installs solutions for security breaches from suppliers in a timely manner. All this only if and insofar the relevant software has been/is delivered, used, or maintained by the Processor for the benefit of the Controller.

13. Procedures are in place for timely and effective treatment of incidents with information security and vulnerabilities in security as soon as they are reported.

14. The Controller reports Data Breaches that are subject to a regulatory reporting obligation to the relevant supervising authority (usually the Data Protection Authority