Renaissance

Data Processing Agreement version 1.1

The undersigned:

1. **(COMPANY NAME),** established in _____, registered at the Chamber of Commerce under number _____, hereinafter referred to as "Data Controller", on the one hand,

   and

2. ***RENAISSANCE IT*,** established in *Rijswijk*, registered at the Chamber of Commerce under number 28078857, hereinafter referred to as "Processor", on the other hand,

Hereinafter also to be jointly referred to as 'the Parties' and individually as 'the Party'.

Considerations

- The parties have agreed in the Principal Agreement that Processor will provide certain services to the Data Controller.
- Processor will process personal data (hereinafter referred to as "Personal Data"), in the context of the Principal Agreement, for the purpose of Personal Data Processing within the meaning of the General Data Protection Regulation (Regulation 2016/679 / EU, hereinafter referred to as the "AVG").
- Parties in this Data Processing Agreement - also pursuant to Article 28 of the AVG - wish to capture a number of conditions which apply to their relationship in relation to the given data processing services, which are provided by the processor.

Parties declare to have agreed as follows:

1. DEFINITIONS

1.1. Concerned:
The natural person, to whom the Personal Data relate.

1.2. Processor:
The natural person or legal entity that processes Personal Data on behalf of the Data Controller without being subject to direct authority.

1.3. Processing Agreement:
This agreement between Data Controller and Processor on the subject of the processing of Personal Data, including all documents referenced and setting forth the detailed rights and obligations of the Parties.

1.4. Data Breach:
A breach of security measures aimed at protecting Personal Data against loss or any form of unlawful processing of Personal Data, including unauthorized modification of Personal Data.

1.5. Master Agreement:
The agreement which Data Controller and Data Processor have entered into, with regards to the supply of services by the Data Processor and which entails the processing of Personal Data.

1.6. Personal Data:
Any information relating to an identified or identifiable natural person.

1.7. Sub-processor:
Any non-subordinate third party hired by the Processor to help process Personal Data as part of the Agreement, not being Employees.

1.8. Data Controller:
The natural or legal person or any other person, or the administrative body that alone or in conjunction with others, determines the purpose of, and the means for the processing of Personal Data.

1.9. Processing of Personal Data:
Any operation or set of operations which is performed upon Personal Data, at least including the collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other form of posting, assembling, alignment or connection, as well as the blocking, erasure or destruction of Personal Data.

1.10. All of the words and terms used above in the singular shall have the same meaning as in the plural and vice versa.

1.11. The headings above the articles of this Data Processing Agreement are only intended to increase the readability of the Data Processing Agreement. The content and scope of a particular heading included with an article, does not limit it to that designation.

2. PROCESSING OF PERSONAL DATA

2.1. Data Controller will have Personal Data processed by Processor in accordance with Appendix 1. Processor processes Personal Data solely pursuant to the Master Agreement, this Data Processing Agreement and other written instructions agreed upon with the Data Controller. Processor will not use the Personal Data under any circumstances for their own purposes, except for legal requirements otherwise

2.2. Processor is not entitled to engage a sub-processor without the prior written permission of the Data Controller. Processor will inform the Data Controller about proposed changes concerning the addition or replacement of sub-processors. Data Controller will be given the opportunity to object to these changes. In case the Data Controller objects, the Processor is entitled to cancel or suspend the Master Agreement with immediate effect, or the execution thereof, without to be held to any (damage) compensation or other obligation as a result of such termination. In addition, before proceeding to the involvement of the Sub-processor, the Processor will enter into a written agreement with the Sub-processor to impose the same or similar obligations to that Sub-processor as resting on Processor itself under this Data Processing Agreement.

2.3. Data Controller hereby gives Processor consent under Article 2.3 to enable Sub-processors for hosting and technical support purposes. Furthermore, Data Controller gives permission to enable the Sub-processors listed in Appendix 1.

2.4. Processor will assist Data Controller, taking into account the type of processing and the information available to Processor, if necessary and where possible, in meeting the obligations under articles 32 to 36 of the AVG.

2.5. Furthermore, Processor will, taking into account the nature of the processing, and the (technical) capabilities which are immediately available to the Processor, assist Data Controller, to the extent possible, with the discharge of the duty of the Data Controller to answer requests from parties involved concerning the rights of access, correction , restriction, objection or removal of personal data.

2.6. Processor will store and process Personal Data only within the European Economic Area, unless otherwise agreed upon with the Data Controller.

2.7. Processor will provide Data Controller all information necessary to demonstrate compliance with the Data Processing Agreement. For that, Processor will provide support to audits in particular, including inspections, by Data Controller or an auditor, authorized by Data Controller. The cost of such audits shall be borne by the Data Controller.

2.8. Data Controller guarantees that the processing of personal data as instructed to Processor and / or implemented by Data Controller using the services of Processor is not in violation of regulations concerning the protection of Personal Data and is not unlawful. Data Controller indemnifies Processor for all claims of third parties, including regulators, relating thereto.

2.9. If Processor has (to be able) to fulfill any obligation under the Processing Agreement and certain (whether technical) measures, research activities, changes or actions (herein jointly: activities) are required, Processor may only be required to carry out these activities, if expressly agreed in writing with Processor. Processor is entitled to charge prices to Data Controller for the work required in this regard. Below is partly, but not exclusively, meant the time spent by employees of the Processor to comply with Articles 2.4 t / m 2.6 and 4.2.

3. BEVEILIGING

3.1. Processor will take appropriate technical and organizational measures to protect the Personal Data against loss or any form of unlawful processing.

3.2. The measures adopted at the conclusion of the Data Processing Agreement referred to in section 3.1 are listed in Appendix 2. Data Controller recognizes that, with the measures specified in Appendix 2, Processor fulfills the obligation under Article 3.1.

3.3. If, either on the basis of revised laws and / or regulations, further measures prove necessary to be be able to keep on ensuring an appropriate level of security as defined in Article 3.1, Processor is entitled to charge (additional) prices to Data Controller, with regard to the costs incurred by Processor in connection with such further measures, before Processor is obliged to updating to Data Controller.

4. DATALEKKEN

4.1. Data Controller is responsible for assessing the existence of an obligation to, and actual performance of the report of a data breach to a supervisory authority and / or Stakeholders.

4.2. Processor will report any data breach after notice thereof by Processor, as soon as possible to Data Controller. Processor shall include on that occasion, as far as possible, in any event, the following information: For

a) The (presumed) cause and nature of the data breach;

b) The categories of data subjects and Personal Data in question and the approximate number of data subjects concerned;

c) The (as yet known and / or expected) consequences of the data breach.

4.3. At the request of the Data Controller, Processor will contribute to the adequate information of the data subjects or the regulatory bodies about the data breach and will remain available for consultation with the Data Controller.

4.4. Data Controller and Processor maintain strict confidentiality towards everyone other than each other about the data leak, any fears of a data

breach and other related matters, unless otherwise stated under European Union law or Dutch law.

5. SECRECY

5.1. Parties are aware that Personal Data qualify as confidential information and they are required to maintain the confidentiality of Personal Data. Personal Data may only be used pursuant to the Master Agreement and the Data Processing Agreement.

5.2. Processor will not make Personal Data available to others than his own employees and / or third parties who have a legitimate reason to access it. Processor will ensure that its employees and / or third parties who have access to the Personal Data have committed themselves to respected confidentiality.

6. DURATION

6.1. The Data Processing Agreement comes into effect at the time of signing and is valid for the duration of the Principal Agreement.

6.2. After completion of the processing activities, at the request of the Data Controller, Processor will, to the extent possible, erase or return all the personal data to Data Controller and delete existing copies unless storage of the personal data is required according to European law or Dutch law.

7. APPENDICES

7.1. The Appendices of the Data Processing Agreement are an integral part of the Data Processing Agreement. When there is conflict between the Appendices and the Data Processing Agreement, the Data Processing Agreement will prevail.

8. APPLICABLE

8.1. This Processing Agreement is governed by Dutch law.

8.2. Disputes between the parties, which can not be resolved in consultation, will be submitted to the competent Dutch court of The Hague District Court, located in The Hague.

Agreed and signed in duplicate in _____ ,

On behalf of:

(NAME DATA CONTROLLER)

(Signature)

Name

Position

Date:

Place:

(NAME PROCESSOR)

(Signature)

Name

Position

Date:

Place:

Appendix 1 - Processing of personal data

(Forming part of the Data Processing Agreement concluded between Data Controller and Processor regarding processing of Personal Data)

The following categories of Personal Data can be provided to Processor:

- Company
- Name
- Function
- Street
- Postcode
- City
- Country
- E-mail address,
- Telephone fixed
- Telephone mobile
- VAT number
- Commercial Register (Chamber of Commerce number)
- Bank account number *(only if there is a signed SEPA direct debit contract available)*

Purpose of processing

The purpose is to store the personal data exclusively for sending invoices by e-mail or by post to the responsible. No further analysis takes place with regard to personal data, nor is it transmitted to third parties.

Duration of treatment

In principle for the duration of the Master Agreement.

Sub-Processors

The sub-processors referred to in 2.3 for which the Data Controller gives permission are:

- AWS
- Campaign Monitor
- Google
- Mailchimp
- Microsoft
- OCOM
- Registrar.eu
- SIDN
- Spam Experts
- Web Security Solutions

Appendix 2 - technical and organizational security

(Belonging to the Data Processing Agreement closed between Data Controller and Processor regarding the processing of Personal Data)

Security measures at the date of conclusion of the Data Processing Agreement:

The following is a summary of the security measures taken by Processor with regards to the processing of Personal Data on behalf of the Data Controller:

Passwords

- All passwords must meet at least in:
    - At least 8 characters in length;
    - At least 1 uppercase, lowercase, numbers and special characters.
- Passwords are not obliged to periodically change.
- Previous passwords from before the time the AVG comes into effect may deviate from these requirements.
- Because passwords are subject sensitive information, it is standard procedure by Processor to send it to the client via a separate method, for example, the last 4 characters via SMS, WhatsApp or by telephone unless the customer does not explicit want this.
- For storing passwords, Processor internally uses a specially developed service called “1Password for Business” (including 256-bit AES encryption key PBKDF2 strengthening, end-to-end encryption).
- Furthermore Processor revokes access to each vault after the termination of an employment contract and remove the account of the former employee.
- Passwords are stored encrypted in recent Plesk installations.

There are customers who use older Plesk installations. These customers will be informed about it so that they can switch over to the latest Plesk versions

---

Encryption

- (Link)connections to the web Plesk Panel are always encrypted via SSL.
- The connection to the name server management system is always encrypted via SSL.
- The connections to and from the R1Soft CDP backup platform and are encrypted via SSL.

- Connections can be either encrypted or unencrypted POP3, IMAP and SMTP, depending on the settings on the side of the customer.
- If the customer has a valid SSL certificate and has set his or her website in such a way, the customer's connection will be encrypted.
- Plesk access logs will default to one month ago.
- IP addresses, usernames, email addresses, domain names and personal information of the client can be logged in here.
- There is no fixed retention time for mail log files.
- IP addresses, usernames, email addresses, times and server responses can be logged in here.
- There is no fixed retention time for web log files.
- IP addresses, times, requested URLs, HTTP status codes, get query strings, browser information and referrer information is logged by default. However, various other types of information can be logged via error logs, think of: debug log lines or code pleas of the CMS system used by the customer. Here we have no influence.
- There is no fixed retention time for ftp log files.
- IP addresses, user names, and file names are logged in by default here.
- There is no fixed retention time for shell login log files (wtmp). IP addresses, user names, protocol used such as SSH, FTP and time of day are logged in here.

Backups

- R1Soft CDP is by default, the standard backup solution used by Processor. The retention of data with R1Soft CDP can go back up to one year. It is not technically possible to remove specific customer data (retroactively) from recovery point moments.
- If (by Processor or a customer) using existing backup option Plesk, the following applies:
- With a set periodic backup, the retention goes back to what it is set to. For Processor this is a maximum of 6 months, but a customer can deviate from this for his or her own Plesk backup.
- It is possible that the Processor stores its Plesk backup on an (internal) other server for offsite backup. This backup server is only approachable via the Processor its internal network and only then, with a user name and password of a valid system account.
- If the customer makes a one-time backup, retention will be until the moment that the customer removes the backup.
- Plesk backup provides the ability to restrict access to the backup with an optional password.

- Plesk backups are saved on the same server and are not accessible by other Plesk-users or externally.
- It is also possible that the customer chooses to store the Plesk backups remotely (via a remote FTP server). Processor in this case has no influence on these external backups.

Other

- Processor has no influence on the data and procedures used on its own servers (dedicated, vps, co-located) used by customers and resellers
- Although Plesk can store Personal Data, Processor only stores the contact name, company name and email address.
- When terminating a contract, this Plesk data is maintained for 2 weeks by default (with the associated hosting), to be removed thereafter. The 2-week period is intended to give customers the opportunity to migrate things such as mail and the website. If required at the customer's request and at his or her own risk, all data can be terminated immediately within Plesk.