Data processing agreement SimplyCode
Version 1.0.2

Contract parties:

Controller
Shared hosting customer, henceforth to be known as “Controller”.

and

Processor
SimplyCode, having it’s Statutory Seat at Elsterweg 8, Sittard, The Netherlands, represented by Edwin van de Ven, henceforth to be known as “Processor” .

Hereinafter collectively referred to as ‘Parties’ .

Considering that:

On the date that Controller started using Processor’s shared hosting platform, we have made an agreement where Processer will be hosting a business application for Controller. For the implementation of this agreement, normal personal data will be processed.

Controller attaches great value to the protection of these personal data, therefore Controller is responsible for the data Processor will be processing and we capture in this data processing agreement:

1. An overview of the personal data to be processed and the processing targets
2. An overview of security measures
3. The process of reporting data leakages and the information to be provided

In addition to what Processor is and isn’t allowed to do with the personal data.

1 Definitions

The before and after used definitions come from Article 4 of the GDPR and have the following meaning.

personal data means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future;

profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;

pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

filing system means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. 2However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;

consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

main establishment means:

- as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
- as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

representative means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

enterprise means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

group of undertakings means a controlling undertaking and its controlled undertakings;

binding corporate rules means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

supervisory authority means an independent public authority which is established by a Member State pursuant to Article 51;

supervisory authority concerned means a supervisory authority which is concerned by the processing of personal data because:

- the controller or processor is established on the territory of the Member State of that supervisory authority;
- data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
- a complaint has been lodged with that supervisory authority;

cross-border processing means either:

- processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
- processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

relevant and reasoned objection means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

information society service means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council ([1]);

international organization means an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

2 Start, duration and termination

1. This Data Processing Agreement becomes effective from the day Controller starts using Processor's shared hosting platform. Using Processor's shared hosting platform implied Controllers' consent to this Data Processing Agreement.
2. This Data Processing Agreement is entered into for the duration set out in the Agreement, and in the absence thereof, for the duration of the cooperation between the Parties.
3. This Data Processing Agreement may not be terminated in the interim.
4. This Data Processing Agreement may only be amended by the Parties subject to mutual consent.
5. Processor shall provide its full cooperation in amending and adjusting this Data Processing Agreement in the event of new privacy legislation.
6. After termination of this data processing agreement, running obligations like reporting data leakages where personal data belonging to Controller is involved and confidentiality will continue for Processor until all personal data of Controller has been either returned or deleted.
7. After termination, all personal data belonging to Controller or data subjects related to Controller, shall be deleted from Processors' systems within 30 days from operational systems and within 4 months from back-up systems.

3 Processing objectives

1. Processor undertakes to process personal data on behalf of the Controller in accordance with the conditions laid down in this Data Processing Agreement. The processing will be executed exclusively within the framework of the Agreement, and for all such purposes as may be agreed to subsequently.
2. Processor shall refrain from making use of the personal data for any purpose other than as specified by the Controller. The Controller will inform the Processor of any such purposes which are not contemplated in this Data Processing Agreement.
3. All personal data processed on behalf of the Controller shall remain the property of the Controller and/or the relevant Data subjects.
4. The Processor shall take no unilateral decisions regarding the processing of the personal data for other purposes, including decisions regarding the provision thereof to third parties and the storage duration of the data.
5. Appendix 1 specifies which personal information is processed by Processor for what objective(s).

4 Processors obligations

1. The Processor shall warrant compliance with the applicable laws and regulations, including laws and regulations governing the protection of personal data, such as the GDPR.
2. The Processor shall furnish the Controller promptly on request with details regarding the measures it has adopted to comply with its obligations under this Data Processing Agreement and the GDPR.
3. The Processor's obligations arising under the terms of this Data Processing Agreement apply also to whomsoever processes personal data under the Processor's instructions.

5 Security

1. Processor will endeavor to take adequate technical and organizational measures against loss or any form of unlawful processing (such as unauthorized disclosure, deterioration, alteration or disclosure of personal data) in connection with the performance of processing personal data under this Data Processing Agreement.
2. Processor does not guarantee that the security measures are effective under all circumstances. The Processor will endeavor to ensure that the security measures are of a reasonable level, having regard to the state of the art, the sensitivity of the personal data and the costs related to the security measures.
3. Controller will only make the personal data available to the Processor if it is assured that the necessary security measures have been taken. Controller is responsible for ensuring compliance with the measures agreed by and between the Parties.

6 Transmission of personal data

1. Processor may process the personal data in countries outside the European Union. In addition, the Processor may also transfer the personal data to a country outside the European Union provided that such country guarantees an adequate level of protection and it satisfies the other obligations applicable to it pursuant to this Data Processing Agreement and the GDPR.
2. Upon request, the Processor shall notify the Controller as to which country or countries the personal data will be processed in.

7 Engaging of third parties or subcontractors

1. The Processor is authorized within the framework of the Agreement to engage third parties, without the prior approval of the Controller being required. Upon request of the Controller, the Processor shall inform the Controller about the third party/parties engaged.
2. The Processor shall in any event ensure that such third parties will be obliged to agree in writing to the same duties that are agreed between the Controller and the Processor.

8 Allocation of responsibility

1. Processor shall only be responsible for processing the personal data under this Data Processing Agreement, in accordance with the Controller’s instructions and under the (ultimate) responsibility of the Controller. Processor is explicitly not responsible for other processing of personal data, including but not limited to processing for purposes that are not reported by the Controller to the Processor, and processing by third parties and / or for other purposes.
2. Controller represents and warrants that it has express consent and/or a legal basis to process the relevant personal data. Furthermore, the Controller represents and warrants that the contents are not unlawful and do not infringe any rights of a third party. In this context, the Controller indemnifies the Processor of all claims and actions of third parties related to the processing of personal data without express consent and/or legal basis under this Data Processing Agreement.
3. Controller ensures no medical, special or in any way sensitive personal data will be processed by Processor. Processor carries no liability whatsoever for any (highly) sensitive personal data provided by Controller, either intentionally or accidentally.
4. Controller shall be responsible for setting, maintaining and implementing a reasonable duration for the storage of personal data. Processor is explicitly not responsible for setting, maintaining and implementing the duration of storage for personal data.
5. If required by law and/or regulation, Processor shall provide any of Controller’s data as requested by the relevant authority(ies). Any costs incurred by Processor during this process of cooperation with relevant authority(ies) shall be borne by Controller.

9 Duty to report

1. In the event of a security breach and/or the leaking of data the Processor shall, to the best of its ability, notify the Controller thereof without undue delay, after which the Controller shall determine whether or not to inform the Data subjects and/or the relevant regulatory authority(ies). This duty to report applies irrespective of the impact of the leak. The Processor will endeavor that the furnished information is complete, correct and accurate.
2. If required by law and/or regulation, Processor shall cooperate in notifying the relevant authorities and/or Data subjects. The Controller remains the responsible party for any statutory obligations in respect thereof.
3. The duty to report is described in detail in Appendix 3.

10 Handling requests from involved parties

1.1. Where a Data subject submits a request to the Processor to inspect or to improve, add to, change or protect their personal data Processor will forward the request to Controller and the request will then be dealt with by Controller. Processor may notify the Data subject hereof.

11 Non disclosure and confidentiality

1. All personal data received by the Processor from the Controller and/or compiled by the Processor within the framework of this Data Processing Agreement is subject to a duty of confidentiality vis-à-vis third parties.
2. This duty of confidentiality will not apply in the event that the Controller has expressly authorised the furnishing of such information to third parties, where the furnishing of the information to third parties is reasonably necessary in view of the nature of the instructions and the implementation of this Data Processing Agreement, or if there is a legal obligation to make the information available to a third party.

12 Audit

1. In order to confirm compliance with this Data Processing Agreement, Controller shall be at liberty to conduct an audit by assigning an independent third party who shall be obliged to observe confidentiality in this regard. Any such audit will follow Processor’s reasonable security requirements, and will not interfere unreasonably with Processor’s business activities.
2. The audit may only be undertaken when there are specific grounds for suspecting the misuse of personal data, and no earlier than two weeks after Controller has provided written notice to Processor.
3. The findings in respect of the performed audit will be discussed and evaluated by the Parties and, where applicable, implemented accordingly as the case may be by one of the Parties or jointly by both Parties.
4. The costs of the audit will be borne by Controller.

13 Miscellaneous

1. The Data Processing Agreement and the implementation thereof will be governed by Dutch law.
2. Any dispute arising between the Parties in connection with and/or arising from this Data Processing Agreement will be referred to the competent Dutch court in the district where the Processor has its registered office.
3. In the case of any inconsistency between documents and the appendices thereto, the following order of priority will apply:
   - the Agreement;
   - the General Terms of Business of Processor;
   - this Data Processing Agreement;
   - additional conditions, where applicable.
   - logs and measurements taken by the Processor shall be deemed to be authentic, unless the Controller supplies convincing proof to the contrary.

14 Appendixes

14.1 Appendix 1

Overview of data processed and processing objectives

Description of processing activities by Processor
Hosting of a CRM system including required data storage

Processing objectives
Storage of Controller customers database

Controller
Controller as defined in this agreement

Processor
Processor as defined in this agreement

Sub processors
None

Processed personal data
Normal personal data, eg.

- Basic name and address information (First & Last name + email address)
- Class attendance
- Event attendance
- Subscription(s)
- Miscellaneous purchases

Involved data subjects
Customers of Controller, the number of which is expected to be below 5000

Processing location
The Netherlands

Storage terms
Personal data provided by Controller will be stored no longer than 30 days on Processors’ systems after a contract has been terminated.
Controller shall be responsible for implementing a reasonable storage policy.

14.2 Appendix 2

Overview of security measures

Technical security

The server(s) operated by Processor should:

- Have a firewall, configured and active allowing only traffic required for the functioning of the hosted application, system administrator and monitoring.
- An operating system installation (eg. a server installation of a recent Linux distribution) along with only required packages and software. Servers should be installed only with software required for application functionality, security or management to reduce the “attack surface”.
- Have a monitoring system check for unauthorized changes to the users file /*etc/passwd* on Linux systems
- Server log in should only be allowed using certificates, to prevent brute-force password attacks.
- System passwords on the server should be at least 8 characters long and complex (containing at least 1 uppercase letter, 1 lower case letter and 1 number).
- Use HTTPS for secure a secure connection to the application
- Operating system updates should be installed at least once every 3 months.

The application provided by Processor should:

- Use reasonably up to date libraries and components, unless a later version would break application functionality
- Save passwords using strong encryption
- Validate input from forms
- Have a reasonably flexible authorization system allowing Controller to specify which employee will have access to which data.

Organizational security

Processor can in no case:

- Keep Controllers’ data on an unsecured USB-key or USB-drive
- Use a very weak password on his work computer
- Store hosting system passwords in unencrypted files

Processor should:

- Dispose of paper documents containing Controllers’ data by shredding them

14.3 Appendix 3

Data leakage reporting process and information to be reported

In any of the following cases, Processor should report to Controller

- When a technical of physical security issue has been found
- When a security issue concerning personal data has been found
- When personal data has (temporarily) been found accessible to unauthorized third parties

Examples include, but are not limited to:

- A website with login information has been hacked or is accessible to unauthorized third parties
- Loss of a laptop or other electronic device containing personal data
- Emails being sent to a wrong address
- An hacker attacks the server infrastructure
- An internal audit reveals a software vulnerability that could have allowed unauthorized access to personal data

Controller security contact

Unless notified otherwise in writing, Processor will use the billing contact information provided by Controller when the need for security related contact arises.

Reporting data leakages and security incidents

The following information should be included in the report

1. **A summary of the incident: what happened?**
   What happened to which systems? (Include the names of the systems involved)
   Or in case of a breach where it’s unclear, what is most likely to have happened.
2. **What kinds of personal data are involved in the incident?**
   List all information that can or could be used to identify a person
3. **What is the scope of the incident: the data of how many people is involved?**
   Please provide a minimum and maximum number of people.
4. **Describe the group(s) of people who’s data is involved in the incident.**
   Eg. Data of employees, customers, etc. Sensitive groups like children should get special attention
5. **Is the contact information of the people involved known?**
   Can we reach the people involved?
6. **What is the (most likely) root cause of the incident?**
   Do you have any idea what might have caused the incident?
7. **When known, on what date or in which time frame has the incident occurred?**
   Please be as precise as possible.

In case of a technical issue, the following points should be taken into consideration as well

8. **A proposed solution**
   Summary of steps to be taken to resolve the technical issue to prevent future occurrence
9. **Any steps that have been taken towards this solution**
   In case work on a solution has already started, a brief progress report