# DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") reflects the parties' agreement with respect to the terms governing the processing of Personal Data under the Main Agreement and its terms and conditions. This DPA is an addendum to the Master Software as a Services Agreement or "Main Agreement" and is effective upon its incorporation into the Main Agreement, which incorporation may be specified in an Order Form or an executed addendum to the Main Agreement. The Main Agreement means the agreement that concerns the delivery of the MORE OPTIMAL' services (https://www.moreoptimal.com/). The term of this DPA shall follow the term of the Main Agreement. Terms not otherwise defined herein shall have the meaning as set forth in the Main Agreement.

**More Optimal BV**., a company limited by shares, registered in The Netherlands under Chamber of Commerce number 68902107, having its registered place of business at Parallelweg 27, 5223 AL 's-Hertogenbosch, The Netherlands, further mentioned as "***Processor***", and the Customer (as further specified in the Main Agreement) hereinafter referred to as "***Controller***". Processor and Controller are hereinafter also referred to individually as "***Party***" or collectively as "***Parties***"

**Whereas:**

- Under the Agreement, the Processor provides the Services as provided under the Main Agreement to the Controller and in the context of these services, Processor will process (personal) data on Controller's behalf.
- Pursuant to article 28 of the GDPR, Parties wish to enter into this agreement in order to stipulate the conditions applicable to their relationship regarding the aforementioned activities on behalf of Controller.
- For the process of enrolment verification both parties will be regarded as (separate) controllers. A controller to controller statement is agreed to each time the institution wants to access the personal data needed for enrolment verification.

**The Parties agree as follows:**

## Article 1 Definitions

1.1 In this agreement, the following terms indicated with a capital, whether single or plural, will have the following meaning:

a) *Attachment*: An attachment to this Data Processing Agreement that is an inextricable part thereof;

b) *GDPR*: The General Data Protection Regulation (*2016/679/EU*);

c) *Personal Data*: Data which is directly or indirectly traceable to a natural person as defined in article 4(1) of the GDPR;

d) *Processing*: Any act in relation to Personal Data as defined in article 4(2) of the GDPR.

e) *DPA*: this agreement between the Controller and the Processor;

1.2 The terms Controller and Processor shall have the same meaning as provided in article 4 of the GDPR.

1.3 Any other terms that occur both in this agreement, as well as the GDPR, shall have the meaning prescribed to them in article 4 of the GDPR.

## Article 2 Controller and Processor of the Personal Data (article 24, 28 and 29 GDPR)

2.1 Processor undertakes to Process the Personal Data under this DPA on behalf of Controller.

2.2 Controller guarantees that the order to Process the Personal Data is in accordance with all relevant and applicable laws and regulations. Controller indemnifies Processor against all damage and costs arising from and/or related to claims of third parties in connection with not fulfilling this guarantee.

2.3 Controller is responsible for the Processing of the Personal Data as described in this DPA.

2.4 An overview of the way the Personal Data is supplied, the categories of Personal Data, the categories of data subjects, the nature and purposes of the Processing is provided in Attachment I to this DPA.

## Article 3 Confidentiality

3.1 Without prejudice to any existing contractual arrangements between the Parties, the Processor will treat all Personal Data as strictly confidential. The Processor shall ensure that all persons authorized to Process the Personal Data are bound to confidentiality.

3.2 These obligations will not prevent a Party from sharing information with a third party to the extent such disclosure is mandatory under applicable law.

## Article 4 Technical and organizational measures (article 5.1.f, 28, 32 GDPR)

4.1 Processor shall implement appropriate technical and organizational measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of Processing. Considering the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the Processing and the nature of the data to be protected.

4.2 Processor has provided Controller with a comprehensive, up-to-date data protection and security concept for data Processing under the terms of this DPA in Attachment II. Controller has accepted the measures mentioned in this concept and declares that these measures constitute an appropriate level of security.

**Article 5 Third parties and subcontractors**

5.1 Processor may engage third parties and/or subcontractors for the Processing of Personal Data under this DPA.

5.2 Processor is responsible for these third parties and/or subcontractors and shall impose upon the third parties and/or subcontractors the same conditions, duties and responsibilities as contained in this DPA in accordance with article 28.4 GDPR. In accordance with articles 28.3.d; 28.2 and 28.4 GDPR, Processor shall inform (in writing) Controller of any intended changes concerning the addition or replacement of these third parties and/or subcontractors, providing Controller with the opportunity to object to such changes within one week.

**Article 6 International data transfer (Chapter V GDPR)**

6.1 Countries located inside the EEA will be assumed as having an adequate level of protection due to their obligations to comply with GDPR.

62. Processor shall only transfer Personal Data to a country outside of the European Economic Area (EEA) when either:
a. There is an adequate level of protection of the data (as described in articles 44-50 GDPR) or;
b. without an adequate level of protection if such transfer is allowed or required under applicable law (Article 49 GDPR).

6.3 Processor guarantees that subcontractors will only transfer data outside of the EEA in conformity with article 6.2 of this Agreement.

**Article 7 Information and audit (article 28.3.h GDPR)**

7.1 If Processor believes an instruction of Controller causes a breach with the GDPR or other applicable legislation, it will immediately inform in written Controller. Parties will seek an appropriate solution together in case any external developments endanger the lawfulness of the Processing of Personal Data as described in this Agreement.

7.2 Processor will provide upon Controller’s written request all information reasonably deemed necessary to demonstrate compliance with this DPA.

7.3 Controller has the right to perform an audit of the Processor to determine to what extent the Processor complies with the provisions of this DPA. Such an audit will be performed by an independent third party and will take place at a time agreed upon by both Parties. Controller will bear the costs for the audit.

**Article 8 Cooperation of Processor: Data Breaches and Data Subject Requests (articles 33-34 GDPR)**

8.1 Processor shall notify Controller within 36 hours after it obtains knowledge of a (possible) security incident pertaining to the Processing of Personal Data. In the event of a security incident Processor will offer Controller its reasonable assistance.

8.2 After Processor has obtained knowledge of a security incident as meant in article 8.3 below Processor shall take reasonable measures to mitigate the results of the incident as much as possible.

8.3 The term “security incident” as used in this article, includes, but is not limited to:

a) every unauthorized or unlawful Processing, deletion or loss of Personal Data;

b) every breach of the security and/or confidentiality which results in an unlawful Processing, deletion or loss of Personal Data, or any indication that such a breach will occur or already has occurred.

8.4 If Processor receives a complaint or a request (articles 12-23 GDPR) from a natural person regarding the Personal Data (such as a request to access, rectification or erasure), Processor will notify Controller within one week after receiving the complaint or request and will offer Controller its reasonable assistance.

8.5 All notifications made based on this article will be directed to the contract details of the contact person of Controller as stated below. Controller is responsible for keeping these contact details up to date and it warrants it will forward changes in the contact details as soon as possible.

**Article 9 Liability (Article 82 GDPR)**

9.1 Processor is responsible for the proper implementation of the technical and organizational measures as set out in this DPA. Processor is not liable if these measures turn out to be insufficient.

9.2 Controller indemnifies Processor against claims of third parties, including Data Protection Authorities, ensuing from the Processing of Personal Data as set out in this DPA.

9.3 Any liability of Processor due to imputable failure to perform the agreement or on any other ground, is governed by the limitation of liability as agreed upon in the Main Agreement between Parties.

**Article 10Term and termination**

10.1 Either Party may, without judicial intervention, terminate this DPA with immediate effect upon the occurrence of any of the following events:

(i) the other Party applies for or is granted a suspension of payments by court order, or any other event due to which that Party loses absolute control of its property;

(ii) a bankruptcy petition is filed against the other Party or if a court of law declares a bankruptcy (or other relevant order) of the other party;

(iii) the other Party discontinues its business and/or goes into voluntary liquidation;

(iv) the other Party commits a breach of any of the provisions of the DPA and, in the event of a remediable breach, if such breach is not remedied within fifteen (15) days of receipt of written notice demanding that the breach be remedied.

10.3 The obligations from this DPA which are by their nature destined to continue after termination accordingly remain in force after termination of this DPA.

10.4 Processor will not store the Personal Data longer than is necessary for the purposes for which the data were collected, in accordance with article 5.1.c GDPR.

10.6 During this term Processor shall, upon the request of Controller, provide Controller with the Personal Data it then Processes in a format as decided on by Processor.

**Article 11 Applicable law and competent court**

11.1 This DPA is governed by the laws specified in the Main Agreement.

11.2 All controversies, disputes or claims arising out of or relating to this DPA will be settled by the court specified in the Main Agreement.

**Appendix I - Details of the processing of Personal Data**

**Categories of personal data:**

Personal data relating to individuals provided to More Optimal via the Services and processed on behalf of and at the directions of the Controller, and can pertain to the following categories of data, as applicable and depending on the Services provided under the Main Agreement:

- Personal and Business Contact information (company, email, phone, physical address)

**Categories of data subjects:**

Data subjects includes the individuals about whom personal data is provided to More Optimal through the Services and processing on behalf of and at the directions of the Controller which can pertain to data relating to the following categories of data subjects, as applicable and depending on the Services provided under the Main Agreement:

- Visitors and users of the Processor’s Platform and/or website(s)
- Data sets that contain personal data and are uploaded to Processor’s Platform and/or website(s)

**Processing operations (nature and purpose of processing):**

The specific processing activities to be carried out by the Processor are depending on the Services as specified under the Main Agreement and its Order Forms.

**Appendix II - Data Protection and Security Concept (Article 4.2)**

Below is a description of the Technical and Organizational measures taken by More Optimal related to article 32 of the GDPR.

1. **Confidentiality**

a) Access Control

i. Measures to prevent unauthorized persons from gaining access to data processing equipment that processes or uses personal data.
Protection by alarm system; Automatic access control system; Smart card / transponder locking system; Motion detectors; Security locks; Key control (key output etc.); Person control at the gatekeeper / reception.

ii. Actions designed to prevent data-processing systems from being used by unauthorized persons.
Assignment of user rights; Password Complexity Policy; Authentication with username / password; Create user profiles; Assignment of user profiles to IT systems; Key control (key output etc.); Person control at the gatekeeper / reception; Use of anti-virus software; Use of a software firewall; Use of a hardware firewall;

Measures to ensure that data subject users can only access data subject to their access rights and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after storage.
Authorization Policy; Number of administrators reduced to the "most necessary"; Log access to applications, especially when entering, changing and deleting data; physical deletion of media before reuse; Logging of annihilation; Administration of rights by system administrator; Password policy incl. Password length, password change; Secure storage of data media; Encryption of media.

b) Separation control

i. Measures to ensure that data collected for different purposes can be processed separately)
Physically separate storage on separate systems or data carriers; Authorization policy; Logical client separation (software side); Sandboxing; Defining database rights; For pseudonymized data: separation of the mapping file and storage on a separate, secure IT system; Separation of productive and test system.
Pseudonymization

ii. Measures to ensure that data protection principles, such as data minimization, are effectively implemented and that the necessary guarantees are included in the processing in order to comply with the requirements of this Regulation. Separation of the mapping file and storage on a separate, secure IT system; The pseudonymisation is included in the process as early as possible; Pseudonymization is practiced whenever possible to protect confidentiality; Appropriate technical and organizational measures are taken to retain the mapping file.

### 1.4 Integrity

a) Relay control

i. Measures to ensure that personal data cannot be illegally read, copied, altered or removed during electronic transmission or during their transport or storage on data carriers, and that it is possible to verify and determine to which places a transfer of personal data takes place Facilities for data transmission is provided. Transfer of data in anonymised or pseudonymised form where possible; Documentation of the recipients of data and the time periods of the planned release or agreed deletion deadlines;

b) Entry control

i. Actions to ensure that it is possible to verify and verify retrospectively whether and by whom personal data has been entered, altered or removed in the computer systems.

Logging of entry, modification and deletion of data; Create an overview that shows with which applications which data can be entered, changed and deleted; Assignment of rights to enter, change and delete data based on an authorization policy; Traceability of input, modification and deletion of data by individual user names (not user groups).

### 1.5 Availability and resilience

a) Availability control

i. Measures to ensure that personal information is protected against accidental destruction or loss.)

Uninterruptible power supply (UPS); Devices for monitoring temperature and humidity in server rooms; Air conditioning in server rooms; Fire and smoke alarm systems; Fire extinguishers in server rooms; Server rooms not under sanitary facilities.

b) Rapid recoverability

i. Measures to ensure that personal information is protected against accidental destruction or loss.
Retain backup in a secure, offsite location; Create a backup & recovery policy.

### 1.6 Procedures for periodic review, evaluation

a) Privacy Management

i. Measures to ensure that the in-house organization is designed to meet the privacy practitioner's specific needs.)
A privacy policy is available; Appointment of a data protection officer; Evidence of the obligation of data secrecy is available; Privacy impact assessments (if required) are performed and logged; There are standards for IT security; the storage of electronic logs is regulated; Log and log files are evaluated regularly; There are regulations on securing the data; Privacy and data protection measures are occasionally controlled unexpectedly.

b) Incident Response Management

i. Measures to ensure that in the event of a data breach, direct information is sent to the client.

Training of employees regarding the detection of a data breach; There is a policy for reporting data breaches to the client; There is an internal incident response management policy.

c) Privacy-friendly pre-sets

i. Measures to ensure compliance with the requirements of data protection by technology (data protection by design) and privacy-friendly default settings (data protection by default)).
Unsubscribe options in all e-mails (easy unsubscribe); Opt-in for all services; DPIA before new processes (where applicable).

ii. Measures to ensure that personal data processed by sub-contractors can only be processed in accordance with the instructions of the client.
Selection of the sub-contractor under due diligence (regarding data security); prior examination and documentation of the technical and organizational measures taken by the sub-contractor; written instructions to the sub-contractor (for example, by order processing contract); Commitment of employees to confidentiality; Sub-contractor has appointed Data Protection Officer; Ensuring the destruction of data after completion of the contract; Effective control rights agreed with the sub-contractor; Ongoing inspection of the contractor and his activities.