**DATA PROCESSING ADDENDUM BETWEEN A CONTROLLER AND A PROCESSOR OF PERSONAL DATA TO CONTRACT DATED ………….20….**

**(CONTROLLER – „MORETHANDIGITAL INTERNATIONAL“)**

Today, ………………………………, the following Data Processing Addendum *(“Addendum”)* was entered into between:

1. **“MoreThanDigital International GmbH”** Baarermattstrasse 6 c/o Helveticorp GmbH 6340 Baar Switzerland by Benjamin Talin in his capacity of Director, *(herein referred to as “****Controller****”)* on one hand, and

2. ……………………………………………………………

 *(herein referred to as „****Supplier****“ or „****Processor****“) on the other hand,*

separately referred to as the *“****Party****”*, collectively referred to as the “**Parties**“*,* taking into account:

(А) The Parties have entered into a Contract dated …………………………………………………… (*“****Contract****”*), in the execution of which an obligation on the Processor to process Personal Data, at the instruction of the Controller and for purposes determined by the Controller, may arise.

(B) When processing personal data, the Parties are obliged to comply with Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data *(herein referred to as the “****Regulation****”),*

(C) The Parties would like to append the Contract with clauses pursuant to the requirements of Art. 28 of the Regulation,

*The Parties agreed to the following:*

**I. DEFINITIONS**

Art.1. The Parties agree that the terms used in this Addendum shall have the following meaning given to them:

1. ***"Controller"*** means ***MoreThanDigital International Gmbh***, which determines the purposes and means of the processing of Personal Data;
2. „***Contract***“ – has the meaning given to in paragraph (A) above;
3. „***Data Subject Request*** – means a request made by the Data Subject to exercise his rights pursuant to the Regulation like right to access, rectification, deletion, to restriction of processing, to portability, to object processing;
4. „***CPDP***“ – Commission for Personal Data Protection;
5. “***Personal Data***” can be any information that may be related to a natural person who is identified, or a natural person who might be identified, directly or indirectly, through the use of one or more specific features or identifiers associated with that natural person. From the point of view of the nature of the information, the term "Personal Data" includes any kind of statement concerning a person. It includes "objective" information and "subjective" information, opinions or assessments. With regard to the form or medium in which this information is contained, the term "Personal Data" includes information in any form, whether alphabetical, digital, graphic, photographic or acoustic. For example, it includes information stored on paper as well as information stored in computer memory.
6. „***Personal Data of the Controller***“ – means the Personal Data provided by the Controller to the Processor in relation to the Contract and subject to this Addendum;
7. „***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 of the Controller, which are transmitted, stored or otherwise processed by the Processor;
8. "***Processing***" means any operation or set of operations carried out with Personal Data, such as the collection, recording, organization, structuring, storage, modification, use, disclosure by transmission and access, arrangement, erasure or destruction. In practice, any activity involving the use of Personal Data in some form may involve the processing of Personal Data;
9. ***„Processor“*** - ………………....................., in his capacity as Processor Processes Personal Data of the Controller on behalf of the Controller;
10. ***„Regulation“*** – has the meaning given to in paragraph (B) above;
11. ***„Data Subject“*** – means a natural person, who is identified or can be identified (directly or indirectly) on the basis of any information which can be treated as personal data.

**II. GENERAL TERMS**

Art.2. The Processor processes personal data of the Controller only on the written instruction of the Controller, subject to the Contact and this Addendum.

Art.3. The duration, purposes and nature of the, exercised by the Processor, Processing, the categories of Data Subjects, and the types of Personal Data of the Controller are contained in *Schedule 1* of this Addendum.

Art.4. Should there be statutory requirements for the Processor to Process Personal Data of the Controller for purposes outside of the ones contained in this Addendum, the Processor is obliged to notify in advance the Controller, unless the relevant statutory requirements preclude this in consideration of the public interest.

**III. CONFIDENTIALITY**

Art.5. (1) The Processor warrants that before making available Personal Data of the Controller to its employees and other representatives of its personnel, he/she shall make sure those representatives:

1. have undergone relevant training in the field of personal data protection;
2. subject to appropriate confidentiality undertakings;
3. comply with the Processor’s internal personal data protection policies related to the protection of Personal Data pursuant to Art.6, p.1, and to apply the relevant technical and organizational measures for the security of the Personal Data, as indicated by the Processor;
4. to be informed that in the performance of the Contract and this Addendum, some Personal Data of its personnel (e.g. names, number, email) appointed as points of contact, shall be provided to the Controller, and if necessary, the Processor shall ensure their consent to such processing.

 (2) The confidentiality section in this Addendum does not revoke any other confidentiality undertakings between the Parties and shall apply in addition to them.

**IV.** **SECURITY MEASURES**

Art.6.(1) The Processor implements and maintains, at his own cost and expense, all necessary technical and organizational measures to guarantee the adequate level of protection of the Personal Data of the Controller, so that the Processing complies with the requirements of the Regulation and that it takes into account the nature, scope, context and purpose of the Processing and the risks from breaching the security of the Personal Data (including risk from unauthorized or unlawful Processing of Personal Data or accidental or unauthorized loss, alteration, disclosure, destruction or damage to the Personal Data), taking into account the state of the art of technical progress and the cost of implementation of such measures. In the performance of this obligation, the Processor shall:

1. adopt Personal Data protection policies, rules and procedures, where the Processor determines the appropriate security measures, including the measures listed in *Schedule №2* at minimum;
2. maintain and warrant a constant level of confidentiality, integrity, availability and resilience of all his information systems, on paper and electronic medium, including any software that processes information and Personal Data;
3. provide appropriate measures for the timely recovery of the availability and access to the Personal Data in an event of physical or technical accident, for example maintaining back-up copies of the Personal Data;

provide periodic inspections and evaluations of the efficiency of the technical and organizational measures.

**V. SUB-PROCESSORS**

Art.7. The assignment of separate Personal Data Processing activities by the Supplier to a sub-processor shall be carried out under the following conditions:

(1) Before providing the Controller’s Personal Data to a sub-processor, the Supplier shall obtain the Controller’s prior written consent, and shall enter into a written contract with the sub-processor. The content of such contract is determined further below.

(2) The Supplier sends a written request to the Controller to provide his Personal Data to a sub-processor. The request shall point to a legal/natural person (name/company, PIN/UIC), the reason for his inclusion as a sub-processor, the categories of Data Subjects, the Processing activities and the period within which the sub-processor will perform them. If the sub-processor is a natural person, the Supplier warrants that the former shall be informed that his Personal Data will be provided to the Controller, and shall obtain his consent for that purpose, if necessary.

(3) The Controller sends a written approval to the Processor in 5 business days from receipt of the request. Should the Supplier receive a written rejection from the Controller, or not receive a response in the abovementioned timeframe, it shall be deemed that a permission was not granted and the Processor has no right to provide the Controller’s Personal Data to this sub-processor.

(4) Any planned changes for the engagement or replacement with other sub-processor, the Supplier is obliged to obtain the prior written consent of the Controller before providing the Controller’s Personal Data to the new sub-processors, applying the same conditions and timeframes as for the prime approval, as described in subsection 3 above.

(5) The Supplier signs a written contract, agreement or an annex to an existing contract with the sub-processor, for which he/she was granted an approval by the Controller, containing terms and conditions regarding the protection of Personal Data. With this contract the sub-processor shall bear responsibilities towards the Supplier equivalent to the obligations of the Supplier towards the Controller pursuant to this Addendum. In particular, the sub-processor shall be obliged to provide sufficient warranty for the implementation of appropriate technical and organizational measures, so that the Processing complies with the requirements of the Regulation, and shall request the prior written consent of the Controller for the provision of Controller’s Personal Data and assignment of separate processing activities from the sub-processor to another sub-processor. The Controller has the right, upon request, to receive from the Supplier a copy of the contract, relevant to the processing of his personal data.

(6) In event that the sub-processor fails to comply with its obligations to protect the Controller’s Personal Data, the Supplier shall remain fully responsible to the Controller for the obligations performed by the sub-processor.

(7) The Controller has a right, at any time, to request from the Supplier to cease providing Controller’s personal data to the sub-processor. In such event, the Supplier shall instruct the sub-processor to return or destroy the Controller’s Personal Data, unless a legislative act requires such data to be stored further.

**VI. DATA SUBJECT REQUESTS**

Art.8. Тhe Processor shall assist the Controller in complying with its obligations to respond to Data Subject Requests through appropriate technical and organizational measures.

Art.9. Should the Data Subject direct its Data Subject Request to the Processor, the Processor shall send it to the Controller, together with all attached documents, no later than 3 (three) business days from receipt of the Data Subject Request.

Art.10. When requested by the Controller, the Processor is obliged to provide necessary cooperation and additional information as needed to comply with the Data Subject Request.

**VII.** **PERSONAL DATA BREACHES**

Art.11. (1) The Processor shall notify the Controller of any Personal Data Breach without undue delay, and in any event no later than 12 hours upon becoming aware of the breach. The notification shall at least contain the following information:

1. description of 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 Controller’s Personal Data records concerned;
2. any information acquired as a result of an investigation into the perpetrators of the Personal Data Breach or the reasons for its occurrence;
3. description of the likely consequences of the Personal Data Breach
4. description of the measures taken by the Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects and to prevent is reoccurrence.

(2) Where, and in so far as, it is not possible for the Processor to provide the Personal Data Breach information at the same time, the information may be provided in phases. If the information cannot be provided in the timeframe set above, the Processor should notify the Controller in writing of the causes for the delay.

(3) Upon request by the Controller, the Processor shall provide, as soon as possible, cooperation and additional information necessary to notify CPDP and the affected Data Subjects, if necessary.

(4) The Processor has no right to publish or disseminate any information relating to the Personal Data Breach without the prior written consent of the Controller (except in fulfillment of statutory obligations).

(5) The Processor cooperates with the Controller cooperation and provides information when the Controller is:

1. drafting the analysis whether Processing of Controller’s Personal Data by the Controller could cause high risk for the rights of the Data Subjects;
2. carrying out a Data Protection Impact Assessment pursuant to Art. 36 Regulation on the processing activities;
3. conducting periodic audits to evaluate whether the Processing is in compliance with this assessment;

consulting the supervisory (CPDP) prior to processing.

**VIII. AUDIT**

Art.12. (1) The Processor provides the Controller with access to all information necessary to demonstrate his fulfillment of his obligations pursuant to this Addendum. In that regard, during the life of this Addendum and for 12 (twelve) months afterwards, the Processor shall provide full cooperation to the Controller, аn auditor or another person authorized by the Controller for the purposes of inspections. The Processor shall provide access, if necessary, to his premises, resources and personnel.

(2) In the event that inappropriate Personal Data security measures are found during an inspection, or a breach of the Regulation or other legislative acts in the field of Personal Data Protection is established, the Processor is obliged to implement appropriate measures to remediate the breach at his own cost and expense, as requested by the Controller.

(3) The Processor warrants that, at the request of the Controller, he will provide such information, documentation and access to resources from his sub-processors pursuant to Art.12. (1) of this Addendum, and will provide for in the contracts with such sub-processors the implementation of appropriate measure, and that remediation of breaches, at the request of the Controller, will be at their cost and expense.

(4) Should the Processor reasonably consider that an instruction by the Controller infringes the Regulation or other legislative acts in the field of Personal Data Protection, the Processor shall immediately notify the Controller in writing and state the reasons for its opinion.

(5) The Processor is not obliged to comply with instructions of the Controller which he deems is unlawful and shall bear the full responsibility for failing to comply with it, including liability for all material and non-material damages, suffered by the latter as a result of such non-compliance.

(6) The Controller has the right to cease providing his Personal Data to the Processor until the breach has been remedied. This will not be considered non-performance of the Contract on behalf of the Controller. In the event the breach has not been remedied for more than 10 (ten) business days, the Controller has the right to terminate the Contract without notice, unless the Processor has sent a reasoned opinion on the unlawfulness of the Administrator's request.

**VII.** **PERSONAL DATA TRANSFERS**

Art.13. (1) The Processor is obliged not to transfer the Controller’s Personal Data in countries outside of the European Economic Area, as well as international organizations based in such countries without the prior written consent of the Controller, unless:

1. The European Commission has found an adequate level of protection pursuant to Article 25(6) of Directive 95/46/EC, or following 24 May 2018, has issued an adequacy decision pursuant to Art. 45 of the Regulation with regards to such countries; or

The Controller and the data recipient are parties to a Personal Data transfer agreement containing the European Commission’s Standard Contractual Clauses, adopted with Commission Decision 2010/87/EU or an equivalent agreement for the transfer of Personal Data, complying with the requirements of applicable Personal Data Protection Legislation.

**VIII. TERMINATION OF PROCESSING ACTIVITIES**

Art.14. (1) Following completion of the Processing activities or after termination of the Contract and within 30 (thirty) days of receipt of a request by the Controller, the Processor shall, at his own cost and expense, destroy or return (at the Controller discretion) all of Controller’s Personal Data, and shall delete all existing copies of documents containing Controller’s Personal Data, including securing the deletion or return of Controller’s Personal Data from his sub-processors, at their cost and expense, unless otherwise provided for in applicable legislation.

(2) Termination of this Addendum or the Contract in full shall not affect or impair the acquired by the Parties rights and the obligations arising for them before the termination.

(3) Termination of the Addendum shall not affect the operation of clauses for which this was expressly agreed or (given their nature and purpose) by default shall continue to operate following termination.

**IX. LIABILITY**

Art.15. (1) In the event that as a result of non-performance of this Addendum or a breach by the Processor or his sub-processor of the Regulation, or other applicable legislation in the field of personal data protection, the Controller suffers material or non-material damages, expressed in payment of:

1. fines and material sanctions imposed by CPDP pursuant to the Regulation;
2. compensations towards Data Subjects;
3. legal expenses for administrative and civil cases (state tax, attorney’s fees and others);
4. expenses to recover lost or damaged personal data,

the Processor owes a refund of the amounts paid by the Controller within 30 (thirty) day of receipt of a request for the refund.

**X. ADDITIONAL PROVISIONS**

Art.16. The Parties explicitly agree that non-performance of this Addendum shall be considered a material breach of the Contract and shall give the right to the Controller to terminate the Contract unilaterally without a notice.

Art.17. This Addendum forms an integral part of the Contract, and all provision from the Contract continue to operate insofar as they do not conflict with the Addendum (including for matters which are not covered by the Addendum, relevant provisions of the Contract shall apply, where appropriate).

Art.18. All communication, notices, requests and all other correspondence in relation to this Addendum shall be in writing and sent by post, courier, notary invitation, email or by hand at the following addresses of the Parties:

To the Controller:

Point of Contact: …………………………..

E-mail: …………………………..

Address: …………………………..

To the Processor:

Point of Contact: …………………………..

E-mail: …………………………..

Address: …………………………..

**For the Supplier/ Processor:**

**Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*……………………………………………………………………….*

*……………………………………………………………………….*

|  |
| --- |
| **SCHEDULE №1 DETAILS OF PROCESSING**to the Data Processing Addendum between a Controller and a Processor to Contract dated ……………… |
| **Description of Processing Activities** |
| ***Duration*** of the Processing | *(E.g. Until termination of the Contract)* |
| ***Subject-matter*** of the Processing | *(E.g. access and use of data entered in an electronic marketing database)* |
| ***Purpose*** of the Processing | *(E.g. marketing services)* |
| **Data Subjects** | **Types of Personal Data** |
| *(****Customers*** *of the Controller)* | *(E.g. two names, email address, phone number, date of birth, address, PIN, IP address of customers, voice data)* |

|  |
| --- |
| **SCHEDULE №2 EXAMPLE MEASURES**to the Data Processing Addendum between a Controller and a Processor to Contract dated ………………. |

|  |
| --- |
| **А. (Example) Measures when processing Personal Data on paper:** |
| * 1. every employee holds documentation that he works with in a secure drawer or case, so that only him and his direct supervisor/manager have access to it;
	2. documentation containing personal data should not be taken outside the office, unless necessary to comply with contractual or statutory obligations or it was not explicitly requested by the data subject;
	3. it is forbidden for employees to copy and photograph documentation on paper, unless it is not necessary for the performance of their employment obligations;
	4. when leaving the workplace in the office, when working with clients and external persons for more than 5 minutes, employees cannot leave documentation containing personal data on their desks; the documentation should be put away and locked in a cabinet where unauthorized persons have no access to them;
	5. documentation is copied, printed, scanned, shredded by the employee who works with the relevant documentation only or by specifically identified employee with an obligation of confidentiality; employees take the documentation from the office machines as soon as possible and are careful not to leave them unclaimed for a long time;
	6. Documentation containing personal data is shredded /destroyed by tearing into small strips on a special machine/; it is forbidden to throw away documentation in the bin, unless it has been shredded or torn by hand in a way so that reproduction of the personal data in the documentation is impossible.
 |
| **B. (Example) Measures when processing Personal Data on electronic media:** |
| 1. Identification / authentication (unique identification (login) for every user in the IT system): e.g. password, smart card, token; passwords should be “strong”, i.e. at least 8 symbols from different kinds; regular password change;
2. Authorization (defining levels of access to the information in the IT system and preliminary control over access to the IT system of individual users);
3. Control over IT operations:
* Tracking of IT operations (recording and storage in log files), including log-ins to and log-outs from the IT system by individual users;
* period reviews of log files;
1. Safety of the IT system:
* antivirus software; firewall software;
* automatic expiry of the IT session after short period of inactivity;
* limited number of unsuccessful attempts to access the IT system;
1. Personal data protection in mobile devices and physical carriers (laptops, USB devices, CD, DVD) through:
* encryption at hardware and software level
* encryption of the individual files
1. Remote transmission of personal data protection
* encryption of the files in an email communication; encryption of the physical carrier (USB devices, CD, DVD); notification about a cryptographic key / password through a separate message and, if possible, through a different communication channel;
1. Protection against accidental loss or alteration of the data:
* against electricity blackouts: UPS;
* provided recovery of the systems in events of interruption; error reporting.
 |