Brandheroes™

DATA PROCESSING AGREEMENT

Between

Brandheroes ApS
CVR: DK37380865
c/o Thomas Bro Hansen
Østervangsvej 12
8900 Randers C
Denmark
Hereinafter ("Data Controller")

And the vendor

Hereinafter ("Data Processor")

Date 23 May 2018

1. Preamble

1.1. The parties have entered into this Data Processing Agreement (hereinafter referred to as "the Agreement") regarding the Data Processor Processing of Personal Data on behalf of the Data Controller.

2. Background

2.1. The Agreement has been entered into in connection with the implementation of the cooperation agreement between the Parties. (Hereinafter the "Main Agreement")

2.2. These terms apply whether the Main Agreement was made online, over the phone, via email or in any other way.

2.3. The Data Controller's instruction to the Data Processor regarding what categories of personal data, categories of data subjects, and the purpose of the processing are further described in the Main Agreement.

3. Purpose

3.1. The data processor may only process personal data for purposes that is a necessity to fulfil its obligations according to the Main Agreement.

4. Data Processor Obligations:

4.1. In the extent that the Data Processor's obligations under the Main Agreement involve processing of personal data, the following applies:

4.1.1. The Data Processor warrants, both now and for the future, to fulfil its obligations according to the current data protection legislation.

4.1.2. The Data Processor may only treat personal data by documented instructions from the Data Controller, including transfer of personal data to third parties, unless otherwise is required by the [European] Community law or national law of the Member States. In such cases, the Data Processor shall notify the Data Controller of this legal requirement before commencing treatment unless the current law prohibits such notification for reasons of important social interests. If the Data Processor is of the opinion that the Data Controller's instructions are in violation of the valid data protection laws, the Data Processor shall immediately inform the Data Controller.

4.1.3. The Data Processor shall implement appropriate technical and organizational arrangements that would be a necessity to ensure sufficient security that the processed information is accidentally or illegally destroyed or lost or reduced. These arrangements must also secure, that the processed information won’t get to unauthorized disclosure, is being misused or otherwise treated in violation of the Danish data protection legislation currently in force. The Data Processor is thus obliged to:

- Introduce login and password procedures as well as set up and maintain firewall and anti-virus software.
- Ensure continued confidentiality, integrity, accessibility and robustness of treatment systems and services.
- Ensure the ability to restore the availability of and access to personal information in time in case of a physical or technical incident.
- Establish a procedure for regular testing, estimation and evaluation of the effectiveness of technical and organizational arrangements to ensure a safe treatment of the information.
- Use pseudonymization and encryption of personal data, when it is relevant.
- Ensure that only employees with a work-related purpose have access to personal data.
- Keep data media properly so that they are not available to third parties.
- Ensure that buildings and systems used in data processing are safe, and that there is only used high-quality hardware and software that is updated on a continuous basis.
- Ensure that samples and waste material are destroyed in accordance with the data protection requirements, following further instructions from the Data Controller. In special cases, determined by the Data Controller, samples and waste material must be retained or returned.

4.1.4. Personal information is confidential and shall remain confidential. The data processor shall ensure that all persons who process personal data have received sufficient instruction and lessons in processing of personal data and have committed themselves to confidentiality.

4.1.5. If the Data Processor processes personal data in another EU / EEA member country than Denmark, the Data Processor shall accordingly comply with the data protection legislation in that country.

4.1.6. The Data Processor is obliged, without undue delay, to inform the Data Controller of operational malfunctions, suspected breach of data security or other irregularities in the processing of personal data. In any event, the Data Processor shall promptly notify the Data Controller of breach of the security that causes or may result in accidental or illegal access to disclosure, destruction, loss or deterioration of personal data. The Data Processor's notification of the Data Controller must contain:

- (a) a description of the nature of the breach of personal data security including, if possible, the categories of data affected and registered

- (b) The Data Processor's recommended arrangements to reduce the negative impact of the security breach
- (c) a description of the identified and likely consequences of the security breach
- (d) a description of what arrangements have been or should be taken to restore the protection of the processed information.
- The Data Controller must be contacted via +4522555352 or tb@brandheroes.com

4.1.7. The Data Processor shall fully assist the Data Controller in the event of a breach of personal data security. This implies, but is not limited to, providing sufficient information and support in:

- (a) restoring personal data security and preventing future use on security
- (b) limiting the impact of the security breach in relative to the affected data subjects
- (c) providing an overview of the potential loss for the Data Controller as a result of the breach of personal data security.

4.1.8. The Data Processor shall, at the request of the Data Controller, provide the Data Controller with sufficient information to ensure that the Data Processor has taken the necessary technical and organizational precautionary measures and that Data Processor complies with the requirements of the current personal data law currently in force. In connection with this, the Data Processor shall assist in the audit performed by the Data Controller or by a Data Responsible designated representative. The Data Controller shall prove to the Data Processor for the time taken in connection with such auditing.

4.1.9. As of 2018, Data Processor will be required to produce a general audit report describing the current level of security, as well as whether the Data Processor complies with the current personal data law at any given time in December. This report must be prepared by an independent third party and comply with the standard for such a report. The audit report is paid by Data Processor and transmitted to the Data Controller by 31 December of each year.

4.1.10. If the Data Processor or a Sub Data Processor that has received personal data receives a request for processing personal data from a data subject, the Data Processor shall promptly forward this request to the Data Controller unless the Data Processor or Sub-Controller has been explicitly instructed by the Data Controller to handle such requests itself.

4.1.11. The Data Processor shall immediately notify the Data Controller of any request for disclosure of personal data by a law enforcement authority, unless applicable law prohibits this.

4.1.12. At the request of the Data Controller, the Data Processor shall help ensure that all necessary and appropriate steps are taken towards handling complaints and accusations of lacking observance of the data protection legislation in force.

5. Transfer data to non-third party

5.1. Unless the Data Processor is required to do so under applicable law, the Data Processor may only transfer data to another data processor or third party if the Data Processor has received prior written instructions or approval from the Data Controller.

5.2. Prior to transferring personal data to a sub data processor, the Data Processor shall ensure:

- that the Data Controller has approved the use of the sub data processor in writing.
- (2) the Data Processor and the Sub-Processor have concluded an agreement ("Subcontracting Agreement") corresponding to the content of this Agreement, in particular as regards the guarantee of the implementation of appropriate technical and organizational agreements.
- (3) that the Data Processing Agreement automatically terminates in case of termination of this Agreement.
- (4) that the Data Processing Agreement must be submitted to and approved by the Data Controller.

6. Changes

6.1. In the event of changes in the Danish Data Protection Act, the Data Controller is entitled to change his instructions to the Data Processor in this agreement with 2 weeks notice by sending new instructions to the Data Processor in writing. The Data Processor is independently responsible for complying with the personal data law currently in force.

7. Validity and termination

7.1. The Agreement will enter into force on the date of its signature and shall remain in full force and effect until the data processor no longer process any personal data on behalf of the data controller.

7.2. In the event of termination of the Main Agreement, the Agreement shall also terminate. However, the Data Processor is bound according to the terms of the Agreement as long as it processes personal data on behalf of the Data Controller.

7.3. In connection with the termination of this agreement, the Data Controller is entitled to request the processed personal data returned to one of the Data Controller selected media. Alternatively, the Data Controller may require that the processed personal data to be deleted.

7.4. If a party is materially in breach of the terms of the Agreement, the opposing party may, by written claim containing a specification of the breach, terminate this contract with immediate effect if the defaulting party has not brought the non-performing relationship to termination within 14 days of receipt of the forwarded claim. The termination of the Agreement also implies the repeal of the Main Agreement.

7.5. The Data Processor shall indemnify the Data Controller for any claim, loss, responsibility, expenses or damage that is a result of the Data Processor's violation of the Agreement.

8. Law and venue

8.1. This agreement is regulated by the Danish law.

8.2. Any claim and dispute arising out of or otherwise connected with the Agreement shall be ruled on by the District Court of Aarhus.

9. Signatures

Date:	Date:
Data Controller (Bandheroes ApS)	Data Processor (Vendor)
______________________________	______________________________
Signature	Signature