DATA PROCESSING AGREEMENT TORENVLIET YAMAHA CENTER AMSTERDAM

THE UNDERSIGNED:

1. The party with which Controller has a partnership / assignment with clients or sales, maintenance and repair of Yamaha products including: outboard engines, ATVs, waverunnners, generators and boats, hereinafter referred to as: ("Controller") and
2. Torenvliet Yamaha Center Amsterdam, a company having is address at Keienbergweg 109, 1101 GG Amsterdam Zuidoost and registered in the Trade Register of the Dutch Chamber of Commerce with the number 33279589 ("**Processor**").

Hereafter jointly referred to as "**Parties**".

WHEREAS:

- Controller offers The controller offers, during which Controller obtains Personal Data (as defined below) of multiple Data Subjects (as defined below);
- Controller requests some forms of data processing to be performed by the Processor (the "**Assignment**");
- The Processor is willing to process the Personal Data for the Controller;
- The Processor will process the Personal Data under the responsibility of the Controller; and
- With regard to Article 28 of the General Data Protection Regulation (the "**GDPR**"), both Parties wish to establish their rights and duties in connection to the processing of Personal Data by the Processor in this agreement.

DECLARE TO HAVE AGREED AS FOLLOWS:

Article 1 - Definitions

GDPR	The General Data Protection including all (Dutch) implementation legislation which is based on the GDPR and the Dutch Personal Data Protection Act (*Wet bescherming persoonsgegevens*) in the case the agreement is entered into before 25 May 25 2018.
Data Subject	The natural person to whom Personal Data relates.
Appendix	The appendix of this agreement, which contains an overview of the Personal Data that the Parties expect to process, the manner in which the Personal Data will be processed, the purposes and means of the processing and the usage and retention periods of Personal Data.
Data Breach	Every situation in which, due to a security incident, Personal Data are unintentionally accessed by an unauthorized person or are lost, destroyed, amended or unlawfully processed.
Assignment	All services which the Processor provides to the Controller and all other forms of collaboration, under which Processor processes Personal Data as defined in the GDPR.
DPIA	Data Protection Impact Assessment as defined in article 35 of the GDPR.
Personal Data	Every Personal Data concerning an identified or identifiable natural person that the Processor obtains during the execution of the Assignment.

Sub Processor Each party that is assigned to process the Personal Data on behalf of the Processor, which the Processor, based on this agreement, is authorized to process for the Controller.

Article 2 – The Data Subjects

1. To be able to execute the Assignment, the Processor processes Personal Data from the Data Subjects. These Data Subjects are the following groups of persons:
   a. Employees who are employed by the Controller.
   b. Visitors of the shop or shops of the Controller.
   c. Visitors of the Controllers' website.
2. Personal Data of other Data Subjects are not processed by the Processor on behalf of the Controller.

Clause 3 – The execution of processing

1. The Processor agrees to execute the Assignment for the Controller under the conditions of this agreement and in compliance with the GDPR.
2. The Controller holds and continues to hold the complete control over the Personal Data. The Processor processes the Personal Data lawfully, fairly and in a transparent manner.
3. The Processor processes the Personal Data exclusively for the purpose of fulfilling the Assignment. The Processor complies with the written instructions of the Controller, in accordance with the purposes and means determined by the Controller in the Appendix and subject to the retention periods mentioned in the Appendix.
4. The Processor does not make use of a Sub Processor unless the Controller gives its written consent to the Processor to do so.
5. The Controller hereby gives the written permission to the Processor to use one or more Sub Processors when processing the Personal Data.
6. The Processor undertakes the Sub Processors to comply with the same obligations as the obligations of the Processor under this agreement.
7. The Processor remains responsible for the correct fulfillment of this agreement.
8. The Processor informs the Controller when the Processor starts sharing Personal Data with a Sub Processor.

Clause 4 - The rights of Data Subjects

1. The Processor ensures that the Data Subject can exercise all his/ her rights deriving from the GDPR and/ or all other applicable laws and regulation.
2. At first request of the Controller, the Processor will perform the following actions as soon as possible, but at least within five working days after the Controller has submitted the request:
   a. To provide the necessary information;
   b. To improve, complete, erase or shield the Personal Data and;
   c. To transfer the Personal Data to the Controller or to a third party which is designated by the Controller.

Clause 5 – Data Protection Impact Assessment

1. In the event the Controller is obliged to perform a DPIA, the Processor supports and cooperates with the Controller in order to comply with the execution of a DPIA.

2. The Processor supports and cooperates with the Controller with the implementation of new (security) measures that must be taken resulting from a DPIA.
3. The Processor will only charge reasonable costs to the Controller for fulfilling these obligations. These reasonable costs do not exceed a maximum of € 90,- per hour.
4. The Processor supports and cooperates with the Controller with the implementation of new (security) measures that have to be taken as a result of further analyses and changes, such as changing (insights into) legislation.

Clause 6 - Security measures

1. The Processor shall implement appropriate technical and organizational measures which are necessary to protect the Personal Data adequately and to keep these Personal Data protected adequately against any kind of loss or any kind of carelessness or any kind of inexpert or unlawful use or processing. The Processor makes sure that the protection adheres to the actual state of the data protection technique.
2. The Processor undertakes, at least, the following measures:
   a. Encryption of digital files containing Personal Data.
   b. Securing networks via Secure Socket Layer (SSL) technology or via technology that has a comparable security level.
3. The Processor guarantees that persons that act under its authority only process the Personal Data in a lawful manner and in compliance with this agreement and the GDPR.
4. If the Processor fails to take appropriate technical and organizational security measures and, consequently, fails to take appropriate measures within a reasonable time, the Controller is entitled without prejudice to its other rights under this agreement and/ or the law to carry out these measures or to have these measures carried out at the expense of the Processor.
5. The Processor will immediately inform the Controller in case of a data breach concerning Personal Data. The Processor will do so as soon as possible, but at least within 96 hours. The Processor does not charge any costs for this.
6. At the request of the Controller, the Processor will provide the Controller with information about the measures being taken to comply with the GDPR and/ or all other relevant laws and regulation, this agreement and all other instructions of the Controller.

Clause 7 – Record of processing activities

1. The Controller shall maintain a record of processing activities under its responsibility. This record contains the name and contact details of the Controller, the purpose of the processing, a description of the categories of Data Subjects and the categories of personal data.
2. The Processor shall maintain a record of processing activities under the Assignment. This record contains the name and contact details of the Controller as well as the Processor, the purpose of the processing on behalf of the Controller, a description of the categories of Data Subjects, the categories of personal data and a description of the technical and organizational security measures.

Clause 8 - Transfer of Personal Data

1. The Processor only processes Personal Data to a third country when:

    a. That third country has an adequate level of protection;
    b. The transfer is subject to appropriate safeguards or;
    c. There is a derogation for a specific situation which allows the transfer of the Personal Data out of the EU.
2. The Processor only transfers Personal Data to countries and/ or organizations that are outside of the EU when the Controller has given its consent for these transfers.
3. The Controller hereby gives its consent for the transfer of Personal Data to (organizations in) the following countries: The United States.
4. The Processor only transfers Personal Data to the countries in paragraph 3 when the requirement from paragraph 1 is fulfilled.
5. The Processor reports the Controller within which country or countries Personal Data are processed. The Processor also reports the Controller when due to a data breach or for any other reason Personal Data is processed erroneously in a third country.

Clause 9 - Confidentiality

1. All Personal Data processed by the Processor is subject to confidentiality towards third parties. The Processor and all persons employed by the Processor and/ or working on behalf of the Processor are obliged to maintain confidentiality of the Personal Data.
2. The Processor ensures that all persons employed by the Processor and/ or working on behalf of the Processor are obliged to observe confidentiality.
3. Confidentiality is not applicable if this agreement provides otherwise and/ or if a statutory provision or judicial judgment requires publication.
4. The Processor will immediately inform the Controller of any request for access, distribution or other form of retrieval and notification of the Personal Data in violation of the confidentiality included in this article. The Processor will do this within 24 hours after the discovery of the breach of confidentiality.

Clause 10 - Duration and termination of this agreement

1. Parties enter into the agreement for an indefinite period of time. The agreement enters into force on 25 mei 2018.
2. Parties can terminate this agreement intermediary by registered letter with a notice period of 3 months.
3. If this agreement ends or is dissolved, the provisions of this agreement with regard to confidentiality, liability, indemnity and all other provisions that by their nature are intended to continue after termination or termination of this agreement shall remain in force.
4. Parties can terminate this agreement with immediate effect by registered letter, in case of:
    a. application by or the provision of a suspension of payments procedure to the other party;
    b. application for bankruptcy by or bankruptcy of the other party; or
    c. liquidation of the other party or non-temporary discontinuation of the company of the other party.

Clause 11 – Removing the Personal Data

1. The Processor shall make all Personal Data available to the Controller at the first request of the Controller, but at the latest within 10 working days after the termination of this agreement or the Assignment.

2. The Processor is obliged to completely and irrevocably erase all Personal Data at the first request of the Controller.
3. As soon as after the termination of this agreement it is certain that the Controller has all Personal Data in a format accepted in writing by the Controller, the Processor will erase all Personal Data completely and irrevocably within 14 days.
4. The Processor may deviate from the obligations under paragraph 1 and paragraph 2 of this article in the event Personal Data must be retained during a statutory retention period or if it is necessary for it to prove the fulfilment of its obligations to Controller.

Clause 12 – Liability

The Processor is liable for and indemnifies the Controller from all damage caused by the Processor and/or its processing of Personal Data which infringes this agreement or the GDPR and/or relevant legislation.

Clause 13 – Audit

1. To monitor the compliance to this agreement the Controller has the right to audit the Processor once a year. The audit can be conducted by the Controller in the event of permission thereto of the Processor or can be conducted by another auditor mandated by the Controller.
2. The costs of the audit are for the account of the Controller, with the exception of the costs of the Processor's personnel accompanying the audit. If the audit shows that the Processor is materially in breach of the agreement, all costs of the audit are for the account of the Processor, without prejudice to the other rights of the Controller. If the Processor is in default, yet the default is not material, the Processor shall repair the default as soon as possible.
3. The Controller will notify the Processor of the audit in writing 10 days before the start of the audit. With this notification the Controller provides the Processor with an explanation of what is to be investigated and how the investigation will take place.
4. In the event the Processor conducts its own audit by an independent certified party, the Processor makes the outcomes of the audit available to the Controller.

Clause 15 – Invalid provisions

If at any time a provision of the agreement is wholly or partially invalid or unenforceable under the applicable legislation and regulations, the other provisions or parts of the provisions of the agreement will continue to apply. The Parties will negotiate in good faith to replace the provision in question with a valid and enforceable provision that differs as little as possible from the original provision in light of the purpose and scope of the agreement.

Clause 16 – Miscellaneous

1. In the event of force majeure, the fulfillment of the obligations arising from or connected with the performance of this agreement for the Party in question will be suspended in whole or in part for the duration of such force majeure, without the Parties being mutually obliged to pay any compensation in this regard.
2. In the event of force majeure, the other party will be notified of this in writing, with the necessary supporting documents.
3. Force majeure means the stipulations in the general terms and conditions of the Processor.

4. This agreement can only be changed in writing by the Parties.
5. The processor is not entitled to suspend the fulfillment of his obligations under this agreement, to set it off or to make it dependent on any action or statement from the Controller. Failure of the Responsible Party to the Assignment or cancellation of the agreement on the basis of which the Assignment is performed can in no way lead to non-compliance with the obligations of the Processor under this agreement.
6. This agreement prevails over all other agreements between the Controller and the Processor.

Clause 17 – Governing law and jurisdiction

1. The agreement, and any non-contractual rights and obligations arising thereto, are completely governed by and will completely be interpreted in accordance with the laws of The Netherlands.
2. All disputes between Parties related to this agreement, or the agreements concluded in the performance of, or in connection with the agreement, will be submitted exclusively to the competent court of Amsterdam.

Article 18 - ANNEXES

Appendix 1: Nature of the data
Appendix 2: Legal and practical security requirements

Appendix 1: Nature of the data

Type of persons involved	Category of data	Origin	Purpose (s) for processing
Customer and supplier contact and its data	- Name - Address - E-mail address - phone number	The customer and its/our suppliers	Executing the agreement, including completing transactions. Checking someone's identity, for example in case of complaints or changes in services. Reporting changes in it policies, documents and our services. Registering and handle complaints, requests and requests. Meet the legal (tax) retention and

			other legal and regulatory obligations.

Appendix 2: Legal and practical security requirements

1. Legal requirements
The Processor will follow the instructions of the Controller with regard to the processing of personal data with regard to applicable laws and regulations and comply with this by taking measures upon request.

2. Practical safety measures
Based on a risk analysis, the Controller must determine which additional measures must be taken to ensure compliance with, among other things, the security policy of the Controller. In principle, these measures must also be implemented before the information exchange of personal data is started.

1. Policy document for information security
A policy document from the Controller is the basis for the quality management system .

1. Allocation and recording of responsibilities for information security
The processor has appointed a person responsible for information security.

2. Classifying personal data
Personal data are confidential and on the basis of the type of personal data this makes demands on security. The controller ensures that the matters relating to personal data are classified.

3. Personnel
Creating awareness and organizing knowledge and training on privacy and security is structurally embedded in the organization of Processor. Staff who come into contact with classified information must sign a confidentiality statement.

4. Access security
Access security consists of physical access and digital access. Rooms where personal data are processed should only be accessible to authorized personnel. Access to systems in which personal data are stored is only possible for authorized personnel using at least a username and password. The Processor has an overview of all authorizations and checks them periodically.

5. Computer and network management
The Processor must take measures to prevent unauthorized access to personal data and that viruses, malware, etc. do not affect the integrity of the personal data.

6. Retention periods
The statutory retention periods for personal data are respected for the Controller.

7. Reporting security incidents
The processor must register all security incidents and inform the Privacy Officer of the Controller in the event of major incidents. Other incidents must be made available to the

Privacy Officer on an annual basis. The Processor must reach the Privacy Officer of the Responsible via the e-mail address: info@yamahacenteramsterdam.nl.

8. Independent research
The processor must cooperate with audits by or on behalf of the Controller.

9. Specific measures

Processor has set the following measures:
· Changes in data or in information processing are only carried out under a change management procedure
· Control of granted powers
· Automatic logging of access to data by employees
· Encryption through encryption of personal data during transmission
· Periodically making backups
· Keeping virus scanners and software up to date