YachtSys Data processing contract

in accordance with article 28 para. 3 of the EU General Data Protection Regulation (GDPR)

between the parties:

Client (controller): User of the software "YachtSys", with following company name and address

……

………..

(in the following called "client")

Contractor (processor): YachtBooker Network AG, ASNP – Hermann Lingg Str. 15, DE 80336 München,

(In the following called "YachtSys" or "contractor")

1. Object and duration of the agreement

The agreement covers the services YachtSys YachtFinder, other YachtSys booking widgets and YachtSys CRM made available to the client through the use of the "YachtSys" software provided by the contractor.

The contractor thereby processes personal data for the client in accordance with Article 4 No. 2 and Article 28 GDPR under the conditions of this contract.

Duration of the contract

The contract shall be concluded for an indefinite period. The contract can be terminated by in the same dates as foreseen in the service contract between the contractor and the client. The client can terminate the contract at any time without notice if the contractor severely violates the data protection regulations or the conditions of this contract, the contractor cannot or refuses to carry out an instruction issued by the client, or the contractor denies the client its control rights in violation of the contract. Failure to comply with the obligations agreed in this contract and derived from Article 28 GDPR is considered a particularly serious violation.

2. Scope, type and purpose of data collection, processing or usage

YachtSys YachtFinder, other YachtSys booking widgets and YachtSys CRM are part of the centralised reservation system for yacht charter – called YachtSys.

In the YachtFinder and other widgets or the client or final customer on the client's website may insert personal data. Those data are used to create and send to the final customer an offer, option or booking to the final customer.

In case of a booking the client who contracted the advanced package with back office can also use the CRM for after sales activities and allow the final customer to complete the crew list and upload skipper license and other documents.

3. Rights and obligations and the client's authority to issue instructions

The client alone is responsible for assessing the legitimacy of processing in accordance with Article 6 para. 1 GDPR and for safeguarding the rights of the data subjects in accordance with Articles 12 to 22 GDPR. Nevertheless the contractor is obligated to immediately disclose all such requests to the client, so far as they can be recognised as exclusively concerning the client. Changes to the object undergoing processing and procedural changes shall be jointly agreed by the client and the contractor and stated in writing or in a documented electronic format.

In general the client shall give all instructions in writing or in a documented electronic format. Verbal instructions should promptly be confirmed

in writing or in a documented electronic format. As determined under No. 5, the client is entitled to ensure compliance with the technical and organisational measures agreed with the contractor as well as the obligations determined in this contract before the start of processing and at regular intervals thereafter, as is reasonable. The client shall immediately inform the contractor if a mistake or irregularity is determined during auditing of the order outcome. The client is obligated to treat all knowledge obtained within the scope of the contractual relationship about the contractor's trade secrets and data protection measures confidentially. This obligation remains unchanged after the termination of this contract.

Normally the client will not need to issue any instruction to the contractor in those matters since he has in YachtSys CRM tools to delete personal data of his customer according to his rules. Once the client deletes customer data, they are also deleted from the contractor's online storage and after the second monthly back up also from all back up files of the contractor.

4. Persons authorised by the client to issue instructions, recipients of instructions on behalf of the contractor

Persons authorised by the client to issue instructions are listed in annex 2.

Recipients of instructions on behalf of the contractor are:

Jens Biermann, CEO, jens@yachtsys.com, +49 89 716774380

Communication channels to be used for instructions:

E-Mail:

Jens@yachtsys.com

Phone:

+49 89 716774380

Address:

YachtBooker Network AG
ANSP – Hermann-Lingg-Str. 15
80336 Munich
Germany

If the contact partner changes or is unavailable for an extended period, the successor to the position or the appropriate representative shall immediately inform the contractual partners either in writing or electronically. The instructions are to be saved for the duration of their validity and for a subsequent three calendar years thereafter.

5. Obligations of the contractor

The contractor processes personal data exclusively within the scope of the concluded agreements and according to the instructions of the client, so far as he is not liable to another processing order under Union or Member State law to which the processor is subject (e.g. investigations of criminal prosecution or state protection authorities); in such a case, the processor shall inform the controller of these legal requirements before processing, unless that law prohibits such information on important grounds of public interest (Article 28 (3) 2 lit. a GDPR).

The contractor shall not use the personal data provided for processing for any other objective, in particular for his own purposes. Copies or duplicates of the personal data shall not be created without the knowledge of the client.

The contractor pledges to implement all agreed measures regarding the ordered processing of personal data in accordance with the contract. He also guarantees that the data processed for the client shall be strictly separated from other datasets. The data carriers originated by the client or being used for the client shall be specifically identified. Input and output as well as current activities shall be documented.

In fulfilling the rights of the data subjects in accordance with Articles 12-22 GDPR, when creating records of processing activities as well as for required data protection impact assessments of the client, the contractor must cooperate to the necessary extent and provide the client with appropriate support, insofar as this is possible (Article 28 (3) 2 lit e and f GDPR). In each case he must immediately forward the necessary information to the client.

The contractor shall immediately inform the client if he believes that an instruction issued by the client is in violation of the legal requirements (Article 28 (3) 3 GDPR). The contractor is entitled to suspend the implementation of the relevant instruction until it is approved or amended by the client, represented by the controller, following an audit.

The contractor must report, delete or limit the processing of personal data gained from the contractual relationship if the client asks this of him by means of an instruction and the legitimate interests of the contractor are not in opposition to this.

The contractor may only pass on information relating to personal data gained from the contractual relationship to third parties or data subjects after receiving prior instruction or agreement from the client. The contractor hereby agrees that the client - principally by appointment - is entitled to monitor compliance with the obligations regarding data protection and data security and compliance with the contractual agreement to an appropriate and necessary extent, either personally or through a third party mandated by the client. Monitoring is carried out in particular by collecting information and inspecting the saved data and the data processing programme, as well as through audits and inspections on site (Article 28 (3) 2 lit. h GDPR).

The contractor guarantees that he shall cooperate with these controls as far as is necessary. The following is hereby agreed until further notice:

The contractor confirms that he is aware of the relevant data protection regulations for order processing included in the GDPR.

The contractor undertakes to protect the confidentiality of the client's personal data during the processing carried out within the order. This remains in effect after the termination of the contract. The contractor guarantees that the employees tasked with carrying out the work are familiar with the data protection regulations which they are governed by before the start of operations, and that they are obliged to observe confidentiality in the appropriate way for the duration of their work as well as after the conclusion of the employment relationship (Article 28 (3) 2 lit. b and Article 29 GDPR).

The contractor shall monitor compliance with the legal data protection requirements within its operations.

An in-house data protection officer is not appointed by the contractor, as there is no legal requirement for such an appointment.

The contractor undertakes to immediately inform the client about suspension from approved codes of conduct in accordance with Article 41 (4) GDPR and the withdrawal of certification in accordance with Article 42 (7) GDPR.

6. Disclosure obligations of the contractor in the event of disruptions in processing and breaches in the protection of personal data

The contractor shall immediately disclose to the client any disruptions or violations committed by the contractor or by persons employed by him, including against data protection regulations or the agreements established in the contract, as well as any suspected data protection violations or irregularities in the processing of personal data. This applies particularly to the potential notification and communication obligations of the client in accordance with Article 33 and Article 34 GDPR. The contractor pledges to adequately support the client in his obligations where necessary, in accordance with Articles 33 and 34 GDPR (Article 28 (3) 2 lit. f GDPR). The contractor may only implement notifications for the client in accordance with Article 33 or Article 34 GDPR after receiving prior instruction as defined in clause 4 of this contract.

7. Relationships with subcontractors (Article 28 (3) 2 lit. d GDPR)

The contractor is only permitted to commission subcontractors to process data belonging to the client with the client's authorisation, Article 28 para. 2 GDPR, which must be gained via one of the aforementioned communication channels (Clause 4) with the exception of verbal permission. Approval can only be granted if the contractor informs the client of the name, address and planned activities of the subcontractor. In addition, the contractor must make certain that he selects the subcontractor carefully, giving particular consideration to the suitability of the technical and organisational measures adopted by this subcontractor in accordance with Article 32 GDPR. The relevant inspection documents shall be made available to the client upon request.

Subcontractors in third states may only be commissioned if the particular requirements of Article 44 GDPR are fulfilled (e.g. adequacy decision by the Commission, standard data protection clauses, approved codes of conduct).

The contractor must contractually ensure that the regulations agreed between the client and the contractor are also valid with respect to the subcontractor. In the contract with the subcontractor, the information shall be precisely stipulated as such that the controllers for the contractor and the subcontractor are clearly distinguished from one another. If multiple subcontractors are used, this extends to the controllers between these subcontractors.

In particular the client must be able to carry out adequate audits and inspections of subcontractors if necessary, including on site, either personally or through the employment of a third party.

The contract with the subcontractor must be concluded in writing, which can also take place in an electronic format (Article 28 (4) and (9) GDPR).

It is only permissible to forward data to the subcontractor if the subcontractor has fulfilled the requirements laid out in Article 29 and Article 32 (4) GDPR with respect to his employees.

The contractor must monitor compliance with the subcontractor(s)' obligations as follows:

The result of the audit shall be documented and made accessible to the client upon request. The contractor shall bear liability to the client for the subcontractor's compliance with data protection regulations which were contractually imposed upon him by the contractor in accordance with the present section of the contract.

As a user, the client agrees to the employment of the following subcontractors:

Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany. (dedicated server and back up server on which YachtSys application is running)

S.C. IOmundo S.R.L. Albinet Street, 36, 700142, Iasi, Romania (development company founded by the contractor which is responsible for the creation, maintenance and regular evolution of YachtSys application)

The processor shall always inform the controller of any planned changes relating to the involvement of new subcontractors or the replacement of former subcontractors, whereby the client retains the ability to object to such changes (§ 28 (2) 2 GDPR).

8. Technical and organisational measures in accordance with Article 32 GDPR (Article 28 (3) 2 lit. c GDPR)

A level of security appropriate to the risk for the rights and freedoms of the natural persons affected by the processing shall be ensured for the specific order processing.

In addition, the protection objectives laid out in Article 32 (1) GDPR such as confidentiality, integrity and availability of systems and services as well as their resilience in relation to the type, scope, conditions and purpose of processing are taken into account in such as way as to permanently reduce the risk through suitable technical and organisational corrective measures.

The procedures described in the annex 1 relating to regular auditing, assessment and evaluation of the effectiveness of the technical and organisational measures in order to guarantee data protection compliant processing shall be defined as binding.

Decisions which are significant for security concerning the organisation of data processing and the procedures used shall be agreed between the contractor and the client.

So far as the measures adopted by the contractor do not satisfy the requirements of the client, the contractor shall immediately inform the client.

In the course of the contractual relationship, the measures can be adjusted by the contractor in line with technical and organisational advancement, however they may not fall short of the agreed standards.

The contractor must agree significant changes with the client in a documented format (written, electronic). Such agreements shall be stored for the duration of this contract.

9. Obligations of the contractor after termination of the contract, Article 28 (3) 2 lit. g GDPR

After the conclusion of the contractual work the contractor must delete or destroy/permit the destruction of all collected data, information and compiled processing and usage results in his possession or in the possession of subcontractors and which are associated with the contractual relationship: The deletion or destruction shall be dated and confirmed to the client in writing or in a documented electronic format or done by the client himself inside the login of YachtSys.

10. Liability

Regulated according to Article 82 (1) to (6) GDPR

The responsibility of the contractor should breach the rules laid out in this contract, in particular with regard to compliance with data protection, is limited to the amount of yearly license or rental fee paid by the client for the "YachtSys" application. This limitation applies only for light or normal negligence, but not for gross negligence or acting on purpose.

11. Miscellaneous

Agreements on the technical and organisational measures as well as control and monitoring documents (including on subcontractors) are to be kept by both contractual partners for the duration of their validity and for a subsequent three full calendar years.

For ancillary agreements, the written form or a documented electronic format is necessary.

If the client’s property or personal data for processing is endangered by the contractor due to the measures of third parties (such as through seizure or sequestration), insolvency or settlement proceedings or other events, the contractor must immediately inform the client.

As set out in § 273 of the German Civil Code (BGB), the defence of right to retention shall be ruled out with respect to the data processed for the client and the associated data carriers.

If an individual part of this agreement should become invalid, this shall not affect the validity of the rest of the agreement.

12. Way of conclusion of this contract

Send this contract completed with your data, your stamp and signature via email to info@yachtsys.com. YachtSys will answer to your email confirming the reception of the completed and undersigned contract and in that way the contract is electronical concluded. A signature from YachtSys is not necessary.

For your own records at best store the email you have sent to us with the completed and undersigned contract and our confirmation of reception in your back up. YachtSys will do the same.

…………………………, the …………………………………………………..

………………………………………………………………………………………

Signature and stamp of client

……………………………………………………………………………………….

Name of underwriting person in readable PRINT LETTERS

Annex 1

Technical and organisational measures in accordance with § 32 para. 2 GDPR

Contractor (YachtSys)

1. Physical access control

- documented distribution of keys to employees

2. System access control

- System access is password protected, user access is only given to employees of the contractor; passwords used must meet the minimum length requirement and be regularly updated

3. User access control

- Through regular security updates and backups (in accordance with state of the art technology) the contractor ensures that unauthorised access is prevented.

4. Transmission control

- Deletion of data in accordance with data protection requirements after the conclusion of the order.

- Options for an SSL encrypted data transfer are available.

5. Job control

- Our employees shall undergo regular training in data protection law and they are familiar with the procedural instructions and user guidelines for data processing within the job, including regarding the client’s right to give instruction. The client is informed that all instructions must be give to CEO Jens Biermann who will delegate it to the regarding employee or execute it personally.

6. Availability control

- Backup and recovery concept with a daily backup of all relevant data. Also monthly back ups to a different server

- Competent use of protection programmes (Virus scanner, firewalls, encryption programmes, spam filter).

7. Data protection measures (physical / logical)

- Data will be saved as physically or logically separate from other data.

- Data protection likewise takes place on systems that are logically and/or physically separate.

Hetzner Online GmbH (Subcontractor)

1. Physical access control

- Electronic access control system with recording function

- High security fence around the entire data centre park

- Documented distribution of keys to employees and Colocation customers for Colocation racks (to each client for his Colocation rack exclusively)

- Guidelines on the supervision and identification of guests visiting the premises

- 24/7 staffing of the data centres

- Video surveillance of the entrances and exits, security gates and server rooms

2. System access control

- System access is password protected, user access is only given to employees of the contractor; passwords used must meet the minimum length requirement and be regularly updated

3. User access control

- for the contractor's internal management systems

- Through regular security updates and backups (in accordance with state of the art technology) the contractor ensures that unauthorised access is prevented.

- Audit-proof, compulsory authorisation allocation procedures for employees of the contractor

- The contractor is solely responsible for transmitted data/software with regard to security and updates.

4. Transmission control

- All employees are obligated to maintain data confidentiality in accordance with § 5 BDSG.

- Deletion of data in accordance with data protection requirements after the conclusion of the order.

- Options for an encrypted data transfer shall be made available within the scope of the service description of the main order.

5. Input control

- for the contractorSs internal management systems

- The data shall be inputted or recorded by the client himself.

- Changes to the data shall be recorded.

6. Job control

- Our employees shall undergo regular training in data protection law and they are familiar with the procedural instructions and user guidelines for data processing within the job, including regarding the client’s right to give instruction.

- The terms and conditions contain detailed information on the type and scope of the ordered processing and the use of the client’s personal data.

- Hetzner Online GmbH has appointed an in-house data protection officer and is ensuring their adequate and effective involvement in the relevant operational processes through the data protection organisation.

7. Availability control

- for the contractor’s internal management systems

- Backup and recovery concept with a daily backup of all relevant data.

- Competent use of protection programmes (Virus scanner, firewalls, encryption programmes, spam filter).

- Use of hard disk mirroring on all relevant servers.

- Monitoring of all relevant servers.

- Use of an uninterruptible power supply.

- Sustained active DDoS protection.

- Backup and recovery concept with a daily backup of data according to the services booked in the main order.

- Use of hard disk mirroring.

- Use of an uninterruptible power supply.

- Use of software firewalls and port regulations.

- Sustained active DDoS protection.

8. Data protection measures (physical / logical)

- for the contractor’s internal management systems

- Data will be saved as physically or logically separate from other data.

- Data protection likewise takes place on systems that are logically and/or physically separate.

Iomundo srl (Subcontractor)

1. Physical access control

- documented distribution of keys to employees

2. System access control

- System access is password protected, user access is only given to employees of the contractor; passwords used must meet the minimum length requirement and be regularly updated

3. User access control

- Through regular security updates and backups (in accordance with state of the art technology) the Iomundo ensures that unauthorised access is prevented.

4. Transmission control

- Deletion of data in accordance with data protection requirements after the conclusion of the order.

- SSL encrypted data transfer are made available.

5. Job control

- Iomundo employees shall undergo regular training in data protection law and they are familiar with the procedural instructions and user guidelines for data processing within the job.

6. Data protection measures (physical / logical)

- Data will be saved as physically or logically separate from other data.

- Data protection likewise takes place on systems that are logically and/or physically separate.

Annex 2

Persons authorised by the client to issue instructions. Please indicate name, surname, position in company, email and – optionally – telephone (just to enable the contractor to identify the authorised person based on his phone number in case of an incoming call):

1

2

3

4

Etc.