DATA PROCESSING AGREEMENT

between

Netlife AS

and

_____

AGREEMENT NOT VALID BEFORE DATE 25-05-2018

BETWEEN:

(1) _____, having its registered office at

_____ (the "Controller"); and

(2) Netlife AS (the "Processor"), having its registered office at Brattørkaia 15b, Trondheim.

BACKGROUND

(A) This Agreement is to ensure there is in place proper arrangements relating to personal data passed from the Controller to the Processor.

(B) This Agreement is compliant with the requirements of Article 28 of the General Data Protection Regulation.

(C) The parties wish to record their commitments under this Agreement.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

In this Agreement:

"Data" means personal data passed under this Agreement. See annex C for details about the types of personal data which can be handled under this agreement.

"GDPR" means the General Data Protection Regulation and is also referred to as "Data Protection Laws".

"Services" means software services related to photography purchased by the Controller from the Processor, where the Processor operates and/or hosts the services.

"Customer" means an entity using the Services to provide an online photography service to end users.

"End user" means a person using the photography services offered by a Customer.

2. Data Processing

The Controller is the data controller for the Data and the Processor is the data processor for the Data. The Data Processor agrees to process the Data only in accordance with Data Protection Laws and in particular on the following conditions:

A. The Processor shall only process the Data (i) on the written instructions from the Controller (ii) only process the Data for completing the Services and (iii) only process the Data in countries governed by the GDPR unless explicitly instructed by the Controller.

B. The Processor shall ensure that all employees and other representatives accessing the Data are (i) aware of the terms of this Agreement and (ii) have received comprehensive training on Data Protection Laws and related good practice, and (iii) are bound by a commitment of confidentiality. The confidentiality lasts also after the termination of this Agreement.

C. The Controller and the Processor have agreed to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, complying with Article 32 of GDPR, details of those measures are set out under Part A of the Annex to this Agreement.

D. The Processor shall not involve any third party in the processing of the Data without the consent of the Controller. Such consent may be withheld without reason. If consent is given a further processing agreement will be required.

E. The Processor shall, taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, in so far as this is possible, for the fulfilment of the Controller's obligation to respond to requests from individuals exercising their rights laid down in Chapter III of GDPR – rights to erasure, rectification, access, restriction, portability, object and right not to be subject to automated decision making etc.

F. The Processor shall assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of GDPR – security, notification of data breaches, communication of data breaches to individuals, data protection impact assessments and when necessary consultation with the national data protection authority ("Norwegian Data Protection Authority"), taking into account the nature of processing and the information available to the Processor.

G. The Processor shall at the Controller's choice safely delete or return the Data at any time, allowing for reasonable time to process the Data. It has been agreed that the Processor will in any event securely delete the Data after the end of the Services without undue delay. Where the Processor is to delete the Data, deletion shall include destruction of all existing copies unless a legal requirement to retain the Data exists. Upon request by the Controller the Processor shall provide written confirmation of destruction of all Data.

H. The processor shall make immediately available to the Controller all information necessary to demonstrate compliance with the obligations laid down under this Agreement and allow for and contribute to any audits, inspections or other verification exercises required by the Controller from time to time.

I. The processor shall make arrangements relating to the secure transfer of the Data from the Controller to the Processor. The safekeeping of the Data by the Processor are detailed under Part A of the Annex.

J. The processor shall immediately contact the Controller if there is any personal data breach or incident where the Data may have been compromised.

3. Termination

The Controller may immediately terminate this Agreement on written notice to the Processor. The Processor may not terminate this Agreement without the written consent of the Controller.

Note however that termination of this Agreement without a replacement agreement will void the Processor's right to store and process the Data. This will prevent the Processor from delivering the Services to the Controller.

4. General

A. This Agreement may only be varied with the written consent of both parties.

B. For the purposes of this Agreement the representatives of each party are detailed under Part B of the Annex.

C. This Agreement represents the entire understanding of the parties relating to necessary legal protections arising out of their data controller/processor relationship under Data Protection Laws.

D. This Agreement is subject to Norwegian law and the exclusive jurisdiction of the Norwegian Courts.

E. If the Controller chooses to terminate this Agreement, or demands deletion of data, the Processor shall not be in breach of contract by being unable to deliver agreed Services. The Controller may also still have obligations under contracts of delivery of the Services.

5. Annexes and updates

The following annexes are part of this Agreement:

A. Compliance with Article 32
B. Controller contact details
C. Data Categories
D. Data Processing Details
E. Subprocessors

The Service is constantly evolving, in great part driven by Customer feedback. Minor changes in what data is stored and how data is used may change over time as the system evolves. In this case, the relevant annexes will be updated, and the Controllers will be notified. The Controller is required to provide the Processor with an e-mail address for such notifications.

For substantial changes in what data is stored or how it is processed, a confirmation of consent from the Controller, or an updated data processing agreement will be required.

For changes in the Controller's use of sub-processors, the Controller will send out notification 30 days in advance.

For and on behalf of _____

.....
(Date and signature)

For and on behalf of Netlife AS

.....
Knut Andreas Tefre - CEO

Annex A: Compliance with Article 32

Compliance with Article 32, para 1 of GDPR

Anonymization and aggregated data

Anonymisation and aggregation of anonymized data is used for keeping historic sales statistics available beyond the reasonable time limit for keeping personal data related to orders/sales.

Encryption

Encryption is applied to all personal data while it is being transferred over public network infrastructure like the Internet. All web browser interfaces and APIs are protected by TLS-encryption and certificates. Off site backups are stored on encrypted data storage devices.

Confidentiality

All access to personal data through the web interface and the APIs is protected by authentication and authorisation. Data transfer is protected from eavesdropping and man in the middle attacks by encryption (TLS).

Integrity

All databases and bulk data storage systems used by the service apply automatic checksumming and error correction of all personal data all the way from the server memory (ECC) down to the filesystem level (ZFS).

Availability

The service availability is automatically monitored 24/7 and critical errors generate alerts to the on call operations team. Service unavailability is handled and if necessary escalated to the rest of the team depending on its severity.

Resilience

Personal data is backed up or replicated to off site storage daily. All primary data storage devices have a resilience configuration of at least either 1+1 data device mirroring or N+2 data + parity (RAID 6, RAIDZ2, Reed Solomon or similar).

The data center housing the servers has the following resilience features:

- Redundant power distribution (A+B).
- Redundant battery backup (UPS) for both A+B power channels.
- Standby diesel power generators (including fuel) for handling grid power loss.
- Dedicated connection to the power grid high-tension ring structure.
- Redundant fiber optic internet connections with route diversity from the data center to two different ISP points of presence.
- Redundant local network infrastructure for handling network component failures.
- Redundant power supplies in all servers connected to the A+B power distribution system for handling power supply or power distribution component failures.
- Redundant network connections to all servers for handling network cable or other network component failures.
- Camera monitoring and electronic access control systems. Electronic access control on doors all the way to and including each server rack.
- The data center is housed inside a robust repurposed military bunker.
- Automatic non-destructive fire suppression system.

Data backup

Backups of data are kept in order to guard against data loss due to bugs, unintentional deletion or modification of data. In order to provide sufficient protection, all deleted data may be kept for up to 90 days before they are permanently unrecoverable.

A new backup mechanism is used after May 25th to ensure that individual data can be removed from the backup before 90 days has passed. Data stored before this date is backed up in such as way that deletion of individual data is not feasible within this time frame. The old backup data will be migrated over to the new regime, and this process will be done by May 25th 2019 at the latest.

Updates

This annex may be updated from time to time in order to clarify how the Processor works with Data. Please refer to section 5 of the main Agreement for details.

Annex B: Controller contact details

The Controller Representative shall be

_____

(Full name in capital letters)

_____

(E-mail in capital letters)

_____

(Telephone with country code)

Annex C: Data Categories

This part describes the categories of personal information stored by the system and a high-level description about how the data is used. For a detailed list of personal data being stored and processed, and details regarding the scope of processing, refer to Annex D.

Scope

This annex, and Annex D, list the data which can be processed by our system for any Controller. For some Controllers, only a subset of these data will be stored and processed due to the scope of delivery and enabled functionality.

Registered users

Information about registered users are stored in order to - among other things - provide end users the ability to create accounts, reset passwords, associate photos with their account, and place orders in the Service.

Subject information

To facilitate photography in which subjects are photographed by the Customer, the system can store subject information and contact information for the persons who can access the pictures after photography.

Message history

Automated messages are generated and sent to the End users and the Customers by the service. A log of the such messages is kept for a customizable amount of time to facilitate debugging, billing, and as proof of work. Subprocessors are used for SMS message delivery. The current subprocessor stores SMS message content for 7 days. SMS metadata (excluding text content) is stored for 45 days (legal requirement on current subprocessor).

Subject and group photos

Photos of single subjects and groups of subjects are transferred to the system by the Customer. References connecting the photos to the subjects are stored by the system.

Orders

When end users place orders in the system, data, including delivery address, pictures for printing and updated price list of the time of order will be stored in order for the order to be fulfilled. It will also be stored some time after, to handle consumer complaints and reprints. Less detailed information can be stored longer for statistical purposes, and for the benefit of end users to view their previous activity.

Transactions

Payment transaction metadata related to orders (excluding payment card details) are stored for a customizable period of time.

Customers

For customers, the Service stores contact details for contact persons, and privilege levels for persons with access to restricted systems.

Job

With regards to photo jobs, the Service stored information about contact persons, information about persons with specific roles (booking, review, photographer, retoucher, et), privilege levels for persons with access to restricted systems, and a log of actions performed by the aforementioned persons are kept.

Kiosk

The service stores information about contact person for a photo kiosks, for support and operational purposes.

Log files

The Service keeps several kinds of log files in order to, including but not limited to enabling debugging, security reviews, and investigations regarding complaints of malfunction. These logs may contain non-sensitive personal data, including but not limited to IP addresses. The log files are normally kept for a maximum of 30 days. In cases where the Processor has a need to store log files longer, any personal data in the log files will be removed or anonymized.

Safe Storage

When the Safe Storage functionality is in use, files, thumbnails and associated file metadata are stored until the End user or Customer deletes the files from the service. Metadata also includes grouping picture files into albums.

Tunability

Referring to Annex D, some data is stored for a specific period due to necessity, in order to fulfill functionality. In many cases, data is also kept for a period longer than strictly necessary, from the perspective of the Service itself. The Controller may have many valid reasons for extending the storage time of different categories of data. The Service provides the Controller with settings to tune these time periods. The Service providers defaults for these settings, and it is the responsibility of the Controller to change these if desired or required.

Updates

This annex will be updated when there are changes in the storage or use of Data. Please refer to section 5 of the main Agreement for details.

Annex D: Data Processing Details

This annex will be updated with a detailed list of all personal data processed by the Service.
The content will be a detailed expansion of the sections in Annex C.

Updates

This annex will be updated when there are changes in the storage or use of Data.
Please refer to section 5 of the main Agreement for details.

Annex E: Subprocessors

OMMH Scandinavia AB

OMMH Scandinavia AB (BestSMS), Anckargripsgatan 3, 211 19 Malmö, Sweden. BestSMS is used to provide SMS delivery services.

Updates

This annex will be updated when there are changes in the Processor's use of subprocessors. Please refer to the main Agreement for details.