Data Processing Agreement (DPA)

This Data Processing Agreement ("Agreement") is made and entered into by and between:

Customer Name:

Address:

("Data Controller")

and

Virinco Group AS

Address Grønland 1, 3045 Drammen, Norway.

("Data Processor")

Effective Date: 29 April 2025

1. Definitions

1.1. Personal Data: Any information relating to an identified or identifiable natural person ("Data Subject").

1.2. Processing: Any operation performed on Personal Data, such as collection, recording, storage, alteration, retrieval, consultation, use, disclosure, erasure, or destruction.

1.3. Sub-processor: Any third party engaged by the Data Processor to assist in processing Personal Data on behalf of the Data Controller.

1.4. Applicable Data Protection Laws: All applicable privacy and data protection laws, including the General Data Protection Regulation (EU) 2016/679 (GDPR).

1.5. Annexes 1 to 3 form an integral part of this Agreement.

2. Subject Matter and Duration

2.1. Subject Matter: This Agreement governs the processing of Personal Data by the Data Processor on behalf of the Data Controller in connection with the services provided by the Data Processor.

2.2. Duration: This Agreement remains effective for the duration of the service relationship or until terminated in accordance with its terms.

3. Nature and Purpose of Processing

3.1. Nature of Processing: Processing Personal Data as necessary to deliver the agreed services.

3.2. Purpose of Processing: Limited to the provision of services under the underlying agreement or the written instructions of the Data Controller.

4. Obligations of the Data Controller

4.1. Lawful Processing: The Data Controller confirms lawful collection and necessary consents for all Personal Data.

4.2. Instructions: Instructions to the Data Processor must be lawful and in compliance with Applicable Data Protection Laws.

4.3. Data Subject Requests: The Data Controller handles all Data Subject rights requests under Applicable Data Protection Laws.

5. Obligations of the Data Processor

5.1. Processing on Instructions: Process Personal Data only according to the Data Controller's documented instructions, unless required otherwise by law.

5.2. Confidentiality: Ensure that all personnel authorized to process Personal Data are bound by confidentiality.

5.3. Security: The Data Processor shall implement appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful processing, accidental loss, destruction, or damage, as required by Ensure that all personnel authorized to process Personal Data are bound by confidentiality.

5.4. Assistance to the Controller: Assist the Data Controller with:

- Responding to Data Subject requests.
- Conducting Data Protection Impact Assessments (DPIA) where necessary.
- Notifying the supervisory authority and Data Subjects in the event of a data breach.

5.5. Data Breach Notification: Upon becoming aware of a Personal Data breach, the data processor shall notify the data controller without undue delay. Such notification shall contain, at least:

a. a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b. the details of a contact point where more information concerning the personal data breach can be obtained;

c. its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex 3 all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 (Notification of a personal data breach to the supervisory authority) and 34 (Communication of a personal data breach to the data subject) of Regulation (EU) 2016/679.

6. Sub-processing

6.1. Use of Sub-processors: The Data Processor shall not engage any Sub-processor without prior written authorization from the Data Controller. A current list of authorized Sub-processors is included in Annex 1 of this Agreement.

6.2. Sub-processor Obligations: Where the Data Processor engages a Sub-processor, it shall impose the same data protection obligations as set out in this Agreement through a written contract, ensuring that the Sub-processor provides sufficient guarantees to implement appropriate technical and organizational measures.

7. Data Subject Rights

7.1. The Data Processor shall assist the Data Controller in ensuring the rights of Data Subjects under Applicable Data Protection Laws, including but not limited to access, rectification, erasure, restriction of processing, portability, and objection.

7.2. The Data Processor shall immediately inform the Data Controller if it receives any request directly from a Data Subject relating to the Personal Data processed under this Agreement.

8. Data Retention and Deletion

8.1. Retention Period: The Data Processor shall not retain Personal Data for longer than necessary to fulfil the agreed-upon services unless otherwise required by law.

8.2. Data Deletion or Return: Upon termination of the services or at the written request of the Data Controller, the Data Processor shall, at the Data Controller's choice, either delete or return all Personal Data to the Data Controller, unless legal obligations require its retention.

9. Liability

9.1. The Data Processor shall be liable for any damages arising from its breach of the obligations under this Agreement in accordance with Applicable Data Protection Laws.

9.2. The Data Controller shall be responsible for ensuring that the Personal Data is processed in compliance with GDPR and other relevant laws.

10. Updates to the DPA

Virinco Group reserves the right to update or modify this Data Processing Agreement to reflect changes in legal requirements, best practices, or the addition or replacement of Sub-processors. Any updates will be published on Virinco.com website.
Customers are responsible for reviewing the current version and contacting Virinco Group if they require an updated signed copy.

IN WITNESS WHEREOF, the parties hereto have executed this Data Processing Agreement as of the Effective Date.

For Data Controller: [Customer's Name]

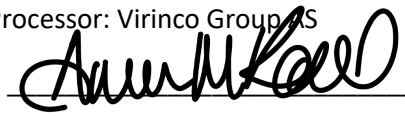
Signature: _____

Name:

Title:

Date: _____

For Data Processor: Virinco Group AS

Signature: 

Name: Anne Monet Røed

Title: Head of Business Operations

Date: 29.04.2025

ANNEX 1: List of Sub-processors

Microsoft Azure
Hosting platform for the WATS Cloud Service
Data handled: Name, email
Location: A WATS instance can be hosted in the Azure West Europe region (Netherlands), the Central US (United States), or Azure East Asia (Hong Kong).
Geo-redundancy with the selected region's paired location, see Azure regional pairs.

ZenDesk
Support services, providing SaaS tool for support ticket handling
Data handled: Name, email, support ticket details
Location: US

Campaign Monitor
Data handled: Name, email, opt-in/out data
Location: US

ChargeBee
Subscription management platform
Data handled: Name, email, subscription details
Location:UK

Pipedrive
CRM
Data handled: Name, email, phone number
Location: The data is primarily hosted in EU data centres, including Stockholm, Frankfurt, and Dublin.

HubSpot
CRM, E-marketing
Data handled: Name, email, phone number, opt-in/out data
Location: Data centres are located all around the world

Xledger
Accounting System.
Data handled: Name
Location: Norway

WATS*
Customer accounts
Name, email, company

*See more info about WATS and where it is hosted, in ANNEX 2 and ANNEX 3.

ANNEX 2: Technical and Organizational Measures

Technical and organisational measures including technical and organisational measures to ensure the security of the data

The technical measures deployed are described in WATS Cloud Security statement. Further details are available in WATS System & Security Documentation.

Excerpt from these documents

- WATS is hosted on Microsoft Azure SaaS/PaaS. A WATS instance can be hosted in Azure West Europe region (Netherlands), Central US (United States) or Azure East Asia (Hong Kong).
- Geo-redundancy with the selected region's paired location, see Azure regional pairs. Encryption is provided in transit using TLS, and at rest using Microsoft Azure storage.
- Authentication can be integrated with Microsoft Azure AD for additional MFA
- Physical security to datacenter is enforced by Microsoft (Azure datacenter)
- Backups are taken on raw data storage and database level as specified in WATS System & Security Documentation.

Organizational security measures are classified as company internal. The internal organizational security policies include the following controls

- Information security policy
- Security incident management
- Asset management
- Access control

ANNEX 3 – Description of the processing in WATS

Categories of data subjects whose personal data is processed

Data subjects are individuals that directly or indirectly have access to WATS or are otherwise appointed contacts or managers of the WATS Subscription

Categories of personal data processed

- General personal data (Full name, e-mail address)
- Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
- No sensitive data is being processed or transferred

Nature of the processing

- The data importer uses full name and email address to identify individual users of the WATS Cloud. Registered users of the application is maintained by subscription owner or manager(s).
- The data importer uses contact information to communicate with the users, and opt-in/out for newsletters and other relevant information.

Purpose(s) for which the personal data is processed on behalf of the controller

- Personal Data is Processed for the purpose of delivering the WATS Cloud service and supporting services.

Duration of the processing

- The data importer will retain Transferred Personal Data until its deletion in accordance with the Master Subscription Agreement (refer to https://wats.com/legal)

For processing by (sub-) processors, also specify the subject matter, nature and duration of the processing as above.