

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: 06. November 2025

1. Definitions

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

1.2. Processing: Any operation or set of operations performed on Personal Data, such as collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, erasure, or destruction.

1.3. Annexes 1 to 3 are an integral part of the Clauses.

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

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

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 shall remain in effect for the duration of the service relationship between the parties or until terminated in accordance with the terms set out herein.

3. Nature and Purpose of Processing

3.1. **Nature of Processing:** The Data Processor will process Personal Data as necessary to provide the agreed-upon services, as detailed in the underlying contract between the parties.

3.2. **Purpose of Processing:** The Data Processor shall only process Personal Data for the purposes of delivering the services defined in the underlying agreement between the Data Controller and Data Processor, or as otherwise instructed by the Data Controller.

4. Obligations of the Data Controller

4.1. **Lawful Processing:** The Data Controller confirms that the Personal Data has been collected in accordance with Applicable Data Protection Laws and that all necessary consents and legal bases for processing are in place.

4.2. **Instructions:** The Data Controller shall ensure that all instructions provided to the Data Processor regarding the processing of Personal Data are lawful and in compliance with Applicable Data Protection Laws.

4.3. **Data Subject Requests:** The Data Controller is responsible for managing all requests from Data Subjects under Applicable Data Protection Laws, including requests for access, rectification, or deletion of Personal Data.

5. Obligations of the Data Processor

5.1. **Processing on Instructions:** The Data Processor shall only process Personal Data per the Data Controller's written instructions unless otherwise required by law. If required by law, the Data Processor will inform the Data Controller of that legal requirement before processing unless prohibited from doing so.

5.2. **Confidentiality:** The Data Processor shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of 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 Article 32 of the GDPR.

5.4. **Assistance to the Controller:** The Data Processor shall assist the Data Controller, by appropriate technical and organizational measures, in fulfilling its obligations regarding:

- 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 may engage Sub-processors to assist in providing the services. A current list of authorized Sub-processors is included in Annex 1 of this Agreement.

For transparency, Virinco clarifies that none of the US-based Sub-processors listed in Annex 1 have access to customer production data or WATS telemetry/test data. Their processing is strictly limited to contact and support information (such as name and email) used for customer support, subscription, and communication purposes.

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 from time to time to reflect changes in legal requirements, best practices, or the addition or replacement of Sub-processors.

Any updates will be published on Virinco Group's 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: DPM - Head of Business Operations

Date: 06.11.2025

ANNEX 1: List of Sub-processors

Microsoft Azure

Hosting platform for the WATS Cloud Service

Data handled: Name, email

Location: EU West region

ZenDesk

Support services, providing SaaS tool for support ticket handling

Data handled: Name, email, support ticket details

Location: US

Campaign Monitor

Newsletters from Virinco Technology

Data handled: Name, email, opt-in/out data

Location: US

ChargeBee

Subscription management platform

Data handled: Name, email, subscription details

Location:UK

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.

Except from these documents

- WATS is hosted on Microsoft Azure SaaS/PaaS platform in EU West region, customers may opt-in for hosting in other Microsoft Azure regions
- 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.