CLOUDIWAY GDPR DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") supplements the CLOUDIWAY Software Support Services Agreement between Customer and CLOUDIWAY, or other agreement between Customer and CLOUDIWAY governing Customer's use of the Services (the "**Agreement**"). To the extent that CLOUDIWAY has access to Personal Data in providing the Services to Customer under the Agreement and/or the GDPR applies to the use by Customer of the CLOUDIWAY Services to process Customer Data, Processor will Process Personal Data in accordance with this DPA. Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this DPA will have the meanings given to them in **Section 13** of this DPA. By continuing to use the CLOUDIWAY Services, Customer agrees to the terms and conditions of this DPA.

1. Data Processing.

1.1 Scope and Roles. This DPA applies when Customer Data is processed by CLOUDIWAY. In this context, CLOUDIWAY will act as "**processor**" to Customer who may act either as "**controller**" or "**processor**" with respect to Customer Data (as each term is defined in the GDPR).

1.2 Customer Controls. The Services provide Customer with a number of controls, including security features and functionalities, that Customer may use to retrieve, correct, delete or restrict Customer Data as described in the Documentation. Without prejudice to **Section 5.1**, Customer may use these controls as technical and organizational measures to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects, including related to rights afforded by Article 28 of the GDPR. These controls shall be appropriate and sufficient to help Customer to respond to requests from individuals to exercise their rights.

1.3 Details of Data Processing are described in the Data Processing Details Form and comprises the following categories.

1.3.1 Subject matter. The subject matter of the data processing under this DPA is Customer Data.

1.3.2 Duration. As between CLOUDIWAY and Customer, the duration of the data processing under this DPA is determined by Customer.

1.3.3 Purpose. The purpose of the data processing under this DPA is the provision of the Services initiated by Customer from time to time.

1.3.4 Nature of the processing: Compute, storage and such other Services as described in the Documentation and initiated by Customer from time to time.

1.3.5 Type of Customer Data: Customer Data uploaded to the Services under Customer's CLOUDIWAY accounts.

1.3.6 Categories of data subjects: The data subjects may include Customer's customers, employees, suppliers and end-users.

1.4 Compliance with Laws. Each party will comply with all Laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR.

2. Customer Instructions.

The parties agree that this DPA and the Agreement (including the provision of instructions via configuration tools made available by CLOUDIWAY for the Services) constitute Customer's documented instructions regarding CLOUDIWAY's processing of Customer Data ("**Documented Instructions**"). CLOUDIWAY will process Customer Data only in accordance with Documented Instructions from Customer, unless required to do so by Union or French law to which CLOUDIWAY is subject. In this case, CLOUDIWAY shall inform Customer of that legal requirement before processing, unless the law prohibits this on the important grounds of public interest. Subsequent instructions may

also be given by Customer throughout the duration of the processing of personal data. These instructions shall always be documented. CLOUDIWAY shall immediately inform Customer if, in CLOUDIWAY's opinion, instructions given by Customer infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions. CLOUDIWAY shall process the personal data only for the specific purpose(s) of the processing, as set out in **Annex 2**, unless it receives further instructions from Customer. CLOUDIWAY shall process the personal data only for the specific purpose(s) of the processing, as set out in **Annex 2**, unless it receives further instructions from the Customer. Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between CLOUDIWAY and Customer, including agreement on any additional fees payable by Customer to CLOUDIWAY for carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if CLOUDIWAY declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA. Processing by CLOUDIWAY of personal data shall only take place for the duration specified in **Annex 2**.

3. Confidentiality of Customer Data.

CLOUDIWAY will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a witness summons or court order). If a governmental body sends CLOUDIWAY a demand for Customer Data, CLOUDIWAY will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, CLOUDIWAY may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Data to a governmental body, then CLOUDIWAY will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless CLOUDIWAY is legally prohibited from doing so. If the Clauses apply, nothing in this Section 3 varies or modifies the Clauses.

4. Confidentiality Obligations of CLOUDIWAY Personnel.

CLOUDIWAY restricts its personnel from processing Customer Data without authorization by CLOUDIWAY as described in the CLOUDIWAY Security Standards. CLOUDIWAY imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

5. Security of Data Processing

5.1 CLOUDIWAY has implemented and will maintain the technical and organizational measures for the CLOUDIWAY Network to ensure the security of the personal data as described in the **Annex 1** and in this **Section 5.1.** This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the data (personal data breach). In particular, CLOUDIWAY has implemented and will maintain the following technical and organizational measures:

5.1.1 security of the CLOUDIWAY Network as set out in **Annex 1, Section 1.1** of the CLOUDIWAY Security Standards;

5.1.2 physical security of the facilities as set out in **Annex 1, Section 1.2** of the CLOUDIWAY Security Standards;

5.1.3 measures to control access rights for CLOUDIWAY employees and contractors in relation to the CLOUDIWAY Network as set out in **Annex 1, Section 1.1** of the CLOUDIWAY Security Standards; and

5.1.4 processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by CLOUDIWAY as described in **Annex 1, Section 2** of the CLOUDIWAY Security Standards

5.1.5 persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, as per **Section 3** above.

5.2 In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

5.3 Customer may elect to implement technical and organizational measures in relation to Customer Data. Such technical and organizational measures include the following which may be obtained by Customer from CLOUDIWAY as described in the Documentation, or directly from a third party supplier:

5.3.1 pseudonymization and encryption to ensure an appropriate level of security;

5.3.2 measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that are being operated by Customer;

5.3.3 measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and

5.3.4 processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by Customer.

5.4 If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("**sensitive data**"), CLOUDIWAY shall apply specific restrictions and/or additional safeguards.

6. Sub-processing.

6.1 Customer agrees that CLOUDIWAY may use sub-processors listed in **Annex 4** to fulfill its contractual obligations under this DPA or to provide certain services on its behalf, such as providing support services including access to customer's email addresses and potentially discussing customer email subject lines, file and site names, and customer domain names. Customer consents to CLOUDIWAY's use of sub-processors as described in this Section. CLOUDIWAY shall specifically inform in writing Customer of any intended changes of that list through the addition or replacement of sub-processors at least three business days in advance, thereby giving Customer sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). CLOUDIWAY shall provide Customer with the information necessary to enable Customer to exercise the right to object.

6.2 CLOUDIWAY will restrict the sub-processor's access to Customer Data only to what is necessary to maintain the Services or to provide the Services to Customer and any End Users in accordance with the Documentation and CLOUDIWAY will prohibit the sub-processor from accessing Customer Data for any other purpose;

6.3 CLOUDIWAY will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the sub-processors that cause CLOUDIWAY to breach any of CLOUDIWAY's obligations under this DPA.

6.4 Where CLOUDIWAY engages a sub-processor for carrying out specific processing activities (on behalf of Customer), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in

accordance with the Clauses. CLOUDIWAY shall ensure that the sub-processor complies with the obligations to which CLOUDIWAY is subject pursuant to the Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

6.5 At the Customer's request, CLOUDIWAY shall provide a copy of such a sub-processor agreement and any subsequent amendments to Customer. To the extent necessary to protect business secret or other confidential information, including personal data, CLOUDIWAY may redact the text of the agreement prior to sharing the copy.

6.6 CLOUDIWAY shall remain fully responsible to Customer for the performance of the sub-processor's obligations. CLOUDIWAY shall notify Customer of any failure by the sub-processor to fulfil its contractual obligations.

6.7 CLOUDIWAY shall agree a third party beneficiary clause with the sub-processor whereby - in the event CLOUDIWAY has factually disappeared, ceased to exist in law or has become insolvent - Customer shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

6.8 Customer retains the right to regularly review any Sub-Processors and withdraw authorization at any time should Customer reasonably believe that the Sub-Processor is not or may not continue to be compliant with Data Protection Laws.

7. Assistance to Customer

7.1 CLOUDIWAY shall promptly notify Customer of any request it has received from the data subject. It shall not respond to the request itself, unless authorized to do so by Customer.

7.2 CLOUDIWAY shall assist Customer in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with **Sections 7(1)** and **7(2)**, CLOUDIWAY shall comply with Customer's instructions.

7.3 In addition to CLOUDIWAY's obligation to assist Customer pursuant to **Section 7(2)**, CLOUDIWAY shall furthermore assist Customer in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to CLOUDIWAY:

7.3.1 the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a "**data protection impact assessment**") where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

7.3.2 the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by Customer to mitigate the risk;

7.3.3 the obligation to ensure that personal data is accurate and up to date, by informing Customer without delay if CLOUDIWAY becomes aware that the personal data it is processing is inaccurate or has become outdated;

7.3.4 the obligations in Article 32 Regulation (EU) 2016/679/.

7.4 The Parties shall set out in **Annex 2** the appropriate technical and organisational measures by which CLOUDIWAY is required to assist Customer in the application of this Clause as well as the scope and the extent of the assistance required.

8. Security Breach Notification.

8.1 In the event of a personal data breach, CLOUDIWAY shall cooperate with and assist Customer for Customer to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679, taking into account the nature of processing and the information available to CLOUDIWAY.

8.2 In the event of a personal data breach concerning data processed by Customer, CLOUDIWAY shall assist Customer:

8.2.1 in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after Customer has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

8.2.2 in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679/, shall be stated in Customer's notification, and must at least include:

8.2.2.1 the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

8.2.2.2 the likely consequences of the personal data breach;

8.2.2.3 the measures taken or proposed to be taken by Customer to address the personal data breach, including, where appropriate, measures 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.

8.2.3 in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

8.3 In the event of a personal data breach concerning data processed by CLOUDIWAY, CLOUDIWAY shall

8.3.1 notify Customer without undue delay after CLOUDIWAY having become aware of the breach. and such notification shall contain:

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

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

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

8.3.2 take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

8.4 CLOUDIWAY Assistance. To assist Customer in relation to any personal data breach notifications Customer is required to make under the GDPR, CLOUDIWAY will include in the notification all available information about the Security Incident that is relevant and necessary for Customer to assess the severity of the Security Incident, to determine Customer's notification obligation and to perform this notification, if necessary.

9. Audits, Documentation and Compliance.

9.1 At Customer's expense, CLOUDIWAY allows Customer to conduct an audit to verify the adequacy of its security measures and CLOUDIWAY's compliance with its obligations under this DPA, as per the audit procedure set forth in **Annex 3**.

9.2 Taking into account the nature of the Services and the information available to CLOUDIWAY, CLOUDIWAY will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation pursuant to Articles 35 and 36 of the GDPR, by providing the information CLOUDIWAY makes available under this Section 9.

9.3 Nothing in this Section varies or modifies the Clauses nor affects any supervisory authority's or data subject's rights under the Clauses.

9.4 The Parties shall be able to demonstrate compliance with the Clauses.

9.5 CLOUDIWAY shall deal promptly and adequately with inquiries from Customer about the processing of data in accordance with the Clauses.

9.6 CLOUDIWAY shall make available to Customer all information necessary to demonstrate compliance with the obligations that are set out in the Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At Customer's request, CLOUDIWAY shall also permit and contribute to audits of the processing activities covered by the Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, Customer may take into account relevant certifications held by CLOUDIWAY.

9.7 Customer may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of CLOUDIWAY and shall, where appropriate, be carried out with reasonable notice.

9.8 The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

10. Transfers of Personal Data.

10.1 Any transfer of data to a third country or an international organisation by CLOUDIWAY shall be done only on the basis of documented instructions from Customer or in order to fulfil a specific requirement under Union or Member State law to which CLOUDIWAY is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.

10.2 Customer agrees that where CLOUDIWAY engages a sub-processor in accordance with **Section 6** of this Data Processing Addendum for carrying out specific processing activities (on behalf of Customer) and those processing activities involve a transfer of personal data within the meaning of Chapter V of GDPR, CLOUDIWAY and the sub-processor can ensure compliance with Chapter V of GDPR by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

10.3 The Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Clauses (or obligations the same as those under the Clauses) will not apply if CLOUDIWAY has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for the lawful transfer of personal data (as defined in the GDPR) outside the EEA. CLOUDIWAY will transfer data outside the EEA only on documented instructions from Customer.

11. **Non-compliance with the Clauses and Termination of the DPA**.

11.1 Without prejudice to any provisions of GDPR, in the event that CLOUDIWAY is in breach of its obligations under the Clauses, Customer may instruct CLOUDIWAY to suspend the processing of personal data until the latter complies with the Clauses or the contract is terminated. CLOUDIWAY shall promptly inform Customer in case it is unable to comply with the Clauses, for whatever reason.

11.2 This DPA shall continue in force until the termination of the Agreement (the "**Termination Date**").

11.3 Customer shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with the Clauses if:

11.3.1 The processing of personal data by CLOUDIWAY has been suspended by Customer pursuant to point (a) and if compliance with the Clauses is not restored within a reasonable time and in any event within one month following suspension;

11.3.2 CLOUDIWAY is in substantial or persistent breach of the Clauses or its obligations under Regulation (EU) 2016/679 ;

11.3.3 CLOUDIWAY fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to the Clauses or to Regulation (EU) 2016/679.

11.4 CLOUDIWAY shall be entitled to terminate the contract insofar as it concerns processing of personal data under the Clauses where, after having informed Customer that its instructions infringe applicable legal requirements in accordance with Section 2 of this DPA, Customer insists on compliance with the instructions.

11.5 At termination of the Agreement, CLOUDIWAY may destroy or otherwise dispose of any of the Customer Data in its possession unless CLOUDIWAY receives, no later than ten days after the effective date of the termination of this agreement, a written request for the delivery to the Customer of the then most recent back-up of the Customer Data. CLOUDIWAY shall use reasonable commercial endeavors to deliver the back-up to the Customer within 30 days of its receipt of such a written request, provided that the Customer has, at that time, paid all fees and charges outstanding at and resulting from termination (whether or not due at the date of termination). Customer shall pay all reasonable expenses incurred by CLOUDIWAY in returning or disposing of Customer Data.

12. Entire Agreement; Conflict.

Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between any other agreement between the parties including the Agreement and this DPA, the terms of this DPA will control, except that the Service Terms will control over this DPA. For the avoidance of doubt, the provisions in the Agreement regarding the governing laws and jurisdiction shall apply to this DPA.

13. Definitions.

Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below:

- "**Clause**s" means the standard contractual clauses between controllers and processors under Article 28(7) of the GDPR .
- "**CLOUDIWAY Network**" means CLOUDIWAY's data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within CLOUDIWAY's control and are used to provide the Services.
- "**CLOUDIWAY Security Standards**" means the security standards attached to the Agreement, or if none are attached to the Agreement, attached to this DPA as **Annex 1**.
- "**Customer**" means you or the entity you represent.
- "**Customer Data**" means the "**personal data**" (as defined in the GDPR) that is uploaded to the Services under Customer's CLOUDIWAY accounts.
- "**EEA**" means the European Economic Area.

- "**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- "**Processing**" has the meaning given to it in the GDPR and "**process**", "**processes**" and "**processed**" will be interpreted accordingly.
- "**Security Incident**" means a breach of CLOUDIWAY's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the date first above written.

CLOUDIWAY SASU

By_____
Name:
Title:

[CUSTOMER NAME]

By_____
Name:
Title:

Annex 1

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the DPA.

CLOUDIWAY Security Standards

Description of the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons.

1. Information Security Program. CLOUDIWAY will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the CLOUDIWAY Network, and (c) minimize security risks, including through risk assessment and regular testing. CLOUDIWAY will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

1.1 Network Security. The CLOUDIWAY Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. CLOUDIWAY will maintain access controls and policies to manage what access is allowed to the CLOUDIWAY Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. CLOUDIWAY will maintain corrective action and incident response plans to respond to potential security threats.

1.2 Physical Security

1.2.1 Physical Access Controls. Physical components of the CLOUDIWAY Network are housed in nondescript facilities (the "Facilities"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

1.2.2 Limited Employee and Contractor Access. CLOUDIWAY provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of CLOUDIWAY or its Affiliates.

1.2.3 Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. CLOUDIWAY also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

2. Continued Evaluation. CLOUDIWAY will conduct periodic reviews of the security of its CLOUDIWAY Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. CLOUDIWAY will continually evaluate the security of its CLOUDIWAY Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

Incident Response Plan
Data Breach Response Plan
Information Security Policy

Annex 2
Data Processing Details

Description of the customer Data to be provided or accessed by CLOUDIWAY: Methods of providing or accessing the Company Data:

The nature and purpose of the processing (the "Subject Matter")

[*Choose and keep the relevant options*]
Migration products : The Platform migrates customer data between Source and Target Systems
Coexistence products :

- The platform synchronizes address books between different systems
- The platform queries and return Free/Busy information between different systems
- The platform routes emails between different systems

The categories of Data Subjects

Employees of the company
Contact objects within mailboxes or global address lists

The type of Personal Data being processed

First and Last names
Email addresses
Employee Mailbox Data
For Mail Migration: All emails, calendar and contacts
For File Migration: All Files, folder names and structure
For Site and Team Migration: All content stored in the sites and teams supported by migration tools
For Coexistence Products: EMail Addresses, Free/busy calendar information, Company Address Book (other contacts, external users, etc.), object ttributes.

Please refer to online product documentation for more specific details and features of the Cloudiway products.

The duration of the processing

The duration of the subscription as set out in an order

The Categories of any recipients of the Personal Data (if any)

Customer's Contacts and other end users including Customer's employees, contractors, customers, prospects, suppliers and subcontractors

Sensitive data processed

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.

Annex 3

Audit Procedure

(a) Customer gives CLOUDIWAY reasonable prior written notice of at least thirty (30) days before any audit or inspection (unless a shorter notice period is required by Privacy Laws, an order of a supervisory authority, otherwise agreed between the parties or in the event of a Data Breach)

(b) Audits or inspections may not be carried out more frequently than once in any twelve-month period (unless required more frequently by Privacy Laws, an order of a supervisory authority, otherwise agreed between the parties or in the event of a Data Breach)

(c) Customer submits to CLOUDIWAY a detailed audit plan at least two weeks in advance of the proposed audit date describing the proposed scope, duration and start date of the audit. CLOUDIWAY shall review the audit plan and provide Customer with any material concerns or questions without undue delay. The parties will then reasonably cooperate to agree a final audit plan

(d) CLOUDIWAY may restrict access to information in order to avoid compromising a continuing investigation, violating law or violating confidentiality obligations to third parties. Any access to sensitive or restricted facilities by Customer is strictly prohibited due to regulatory restrictions on access to other customers' data, although Customer and/or its auditor shall be entitled to observe the security operations center via a viewing window). Customer shall not (and must ensure that its auditor shall not) allow any sensitive documents and/or details regarding CLOUDIWAY' policies, controls and/or procedures to leave the CLOUDIWAY location at which the audit or inspection is taking place (whether in electronic or physical form)

(e) Customer carries out the audit or inspection during normal business hours and without creating a business interruption to CLOUDIWAY

(f) The audit or inspection is carried out in compliance with CLOUDIWAY' relevant on-site policies and procedures

(g) Where the audit is carried out by a third party on behalf of the Customer, such third party is bound by similar obligations to those set out in the Agreement and is not a direct competitor of CLOUDIWAY. CLOUDIWAY reserves the right to require any such third party to execute a confidentiality agreement directly with CLOUDIWAY prior to the commencement of an audit or inspection, and

(h) Except where the audit or inspection discloses a failure on the part of CLOUDIWAY to comply with its material obligations under this DPA, Customer shall pay all reasonable costs and expenses (including

without limitation any charges for the time engaged by CLOUDIWAY, its personnel and professional advisers) incurred by CLOUDIWAY in complying with this clause.

Customer shall provide to CLOUDIWAY a copy of any audit reports generated in connection with an audit carried out under this clause, unless prohibited by applicable law. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of applicable Privacy Laws. The audit reports shall be Confidential Information of the parties.

Annex 4
List of Sub-processors

Customer has authorised the use of the following sub-processors who are also processing the Personal Data in the performance of the Services:

SUPPLIER SUB-PROCESSOR LIST

Entity Name	Sub-processing Activities	Location(s) of Processing
Cloudiway, LLC	Customer Support and Consulting Services	United States
Mindgate	Customer Support and Software Development	Tunisia
H2VM TECHNOLOGY SOLUTIONS COMPANY LIMITED	Software Development, Customer Support	Vietnam
Independent Contractors	Customer Support, Software Development	India
Independent Contractor	Consulting Services	Spain, Mexico