21Vianet

21Vianet Online Services Data Protection Addendum

Last updated November 15, 2022

These commitments are binding on 21Vianet as of November 15, 2022.

**Table of Contents**

[Introduction 3](#_Toc118465775)

[Applicable DPA Terms and Updates 3](#_Toc118465776)

[Electronic Notices 3](#_Toc118465777)

[Prior Versions 3](#_Toc118465778)

[Definitions 4](#_Toc118465779)

[General Terms 5](#_Toc118465780)

[Compliance with Laws 5](#_Toc118465781)

[Data Protection Terms 5](#_Toc118465782)

[Scope 5](#_Toc118465783)

[Nature of Data Processing; Ownership 5](#_Toc118465784)

[Disclosure of Processed Data 6](#_Toc118465785)

[Processing of Personal Data 6](#_Toc118465786)

[Data Security 8](#_Toc118465787)

[Security Incident Notification 9](#_Toc118465788)

[Data Location 9](#_Toc118465789)

[Data Retention and Deletion 9](#_Toc118465790)

[Processor Confidentiality Commitment 9](#_Toc118465791)

[Notice and Controls on use of Subprocessors 10](#_Toc118465792)

[Sensitive Personal Data 10](#_Toc118465793)

[How to Contact 21Vianet 10](#_Toc118465794)

[Appendix A – Security Measures 11](#_Toc118465795)

[Appendix B – Data Subjects and Categories of Personal Data 14](#_Toc118465796)

[Appendix C - Additional Safeguards Addendum 16](#_Toc118465797)

[Attachment 1 – The 2021 Standard Contractual Clauses (Controller to Processors) 17](#_Toc118465798)

[Attachment 2 – European Union General Data Protection Regulation Terms 26](#_Toc118465799)

# **Introduction**

The parties agree that this 21Vianet Online Services Data Protection Addendum (“DPA”) sets forth their obligations with respect to the processing and security of Customer Data and Personal Data in connection with the Online Services. The DPA is incorporated by reference into the Online Services Terms (or successor location in the Use Rights). Separate terms, including different privacy and security terms, govern Customer’s use of Non-21Vianet Products.

In the event of any conflict or inconsistency between the DPA Terms and any other terms in 21Vianet Customer Agreement, the DPA Terms shall prevail. The provisions of the DPA Terms supersede any conflicting provisions of the 21Vianet Privacy Statement that otherwise may apply to processing of Customer Data or Personal Data as defined herein. For clarity, consistent with Clause 5 of the 2021 Standard Contractual Clauses in [Attachment](#attachment) 1, when the 2021 Standard Contractual Clauses are applicable, the 2021 Standard Contractual Clauses (if applicable) prevail over any other term of the DPA Terms.

21Vianet makes the commitments in this DPA to all customers with 21Vianet Customer Agreement. These commitments are binding on 21Vianet with regard to Customer regardless of (1) the Use Rights that is otherwise applicable to any given Online Services subscription, or (2) any other agreement that references the OST.

## **Applicable DPA Terms and Updates**

**Limits on Updates**

When Customer renews or purchases a new subscription to an Online Service, the then-current DPA Terms will apply and will not change during Customer’s subscription for that Online Service.

**New Features, Supplements, or Related Software**

Notwithstanding the foregoing limits on updates, when 21Vianet introduces features, supplements or related software that are new (i.e., that were not previously included with the subscription), 21Vianet may provide terms or make updates to the DPA that apply to Customer’s use of those new features, supplements or related software. If those terms include any material adverse changes to the DPA Terms, 21Vianet will provide Customer a choice to use the new features, supplements, or related software, without loss of existing functionality of a generally available Online Service. If Customer does not use the new features, supplements, or related software, the corresponding new terms will not apply.

**Government Regulation and Requirements**

Notwithstanding the foregoing limits on updates, 21Vianet may modify or terminate an Online Service where there is any current or future law, government requirement or obligation that (1) subjects 21Vianet to any regulation or requirement not generally applicable to businesses operating there, (2) presents a hardship for 21Vianet to continue operating the Online Service without modification, and/or (3) causes 21Vianet to believe the DPA Terms or the Online Service may conflict with any such law, requirement or obligation.

## **Electronic Notices**

21Vianet may provide Customer with information and notices about Online Services electronically, including via email, through the portal for the Online Service, or through a web site that 21Vianet identifies. Notice is given as of the date it is made available by 21Vianet.

## **Prior Versions**

The DPA Terms provide terms for Online Services that are currently available. For earlier versions of the DPA Terms, Customer may refer to https://www.21vbluecloud.com/ostpt/ or contact its reseller or 21Vianet Account Manager.

# **Definitions**

Capitalized terms used but not defined in this DPA will have the meanings provided in the 21Vianet Customer Agreement. The following defined terms are used in this DPA:

“Customer Data” means all data, including all text, sound, video, or image files, and software, that are provided to 21Vianet by, or on behalf of, Customer through use of the Online Service.

“China Laws and Regulations” means the laws and regulations of China that are applicable to this DPA, including without limitation, the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law (i.e., the PIPL as defined below), and any updates thereto.

“Data Protection Requirements” means China Laws and Regulations, GDPR, Local EU/EEA Data Protection Laws, and any applicable laws, regulations, and other legal requirements relating to (a) privacy and data security; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.

“DPA Terms” means the terms in the DPA and any Online Service-specific terms in the Use Rights that specifically supplement or modify the privacy and security terms in the DPA for a specific Online Service (or feature of an Online Service). In the event of any conflict or inconsistency between the DPA and such Online Service-specific terms, the Online Service-specific terms shall prevail as to the applicable Online Service (or feature of that Online Service).

“GDPR” means Regulation (EU) 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).

“Local EU/EEA Data Protection Laws” means any subordinate legislation and regulation implementing the GDPR.

“GDPR Terms” means the terms in [Attachment](#Attachment3) 2, under which 21Vianet makes binding commitments regarding its processing of Personal Data as required by Article 28 of the GDPR.

“Personal Data” means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“PIPL” means the Personal Information Protection Law of People’s Republic of China, effective as of 1 November 2021.

“2021 Standard Contractual Clauses” means the standard data protection clauses (controller-to-processor module) for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission in decision 2021/914/EC, dated 4 June 2021. The 2021 Standard Contractual Clauses are in [Attachment](#attachment) 1.

“Subprocessor” means other processors used by 21Vianet to process Customer Data and Personal Data, as described in Article 28 of the GDPR.

Lower case terms used but not defined in this DPA, such as “personal data breach”, “processing”, “controller”, “processor”, “profiling”, “personal data”, and “data subject” will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether GDPR applies, and, if applicable, any equivalent terms in other Data Protection Requirements. The terms “data importer” and “data exporter” have the meanings given in the 2021 Standard Contractual Clauses.

# **General Terms**

## 

## **Compliance with Laws**

21Vianet will comply with all laws and regulations applicable to its provision of the Online Services, including any security breach notification requirements and Data Protection Requirements. However, 21Vianet is not responsible for compliance with any laws or regulations applicable to Customer or Customer’s industry that are not generally applicable to information technology service providers. 21Vianet does not determine whether Customer Data includes information subject to any specific law or regulation. All Security Incidents (as defined below) are subject to the Security Incident Notification terms below.

Customer must comply with all laws and regulations applicable to its use of Online Services, including laws related to biometric data, confidentiality of communications, and Data Protection Requirements. Customer is responsible for determining whether the Online Services are appropriate for storage and processing of information subject to any specific law or regulation and for using the Online Services in a manner consistent with Customer’s legal and regulatory obligations. Customer is responsible for responding to any request from a third party regarding Customer’s use of an Online Service, such as a request to take down content under China Laws and Regulations or other applicable laws.

# **Data Protection Terms**

This section of the DPA includes the following subsections:

* Scope
* Nature of Data Processing; Ownership
* Disclosure of Processed Data
* Processing of Personal Data
* Data Security
* Security Incident Notification
* Data Location
* Data Retention and Deletion
* Processor Confidentiality Commitment
* Notice and Controls on Use of Subprocessors
* Biometric Data
* How to Contact 21Vianet
* Appendix A – Security Measures
* Appendix B – Data Subjects and Categories of Personal Data
* Appendix C – Additional Safeguards Addendum

## **Scope**

The DPA Terms apply to all Online Services except any Online Services specifically identified as excluded in [Attachment](#attachment) 1 to the OST (or successor location in the Use Rights), which are governed by the privacy and security terms in the applicable Online Service specific terms.

For clarity, the DPA Terms apply only to the processing of data in environments controlled by 21Vianet and 21Vianet's subprocessors. This includes data sent to 21Vianet by Online Services but does not include data that remains on Customer's premises or in any Customer selected third party operating environments.

Previews may employ lesser or different privacy and security measures than those typically present in the Online Services. Unless otherwise noted, Customer should not use Previews to process Personal Data or other data that is subject to legal or regulatory compliance requirements. The following terms in this DPA do not apply to Previews: Processing of Personal Data and Data Security.

## **Nature of Data** **Processing; Ownership**

21Vianet will use and otherwise process Customer Data and Personal Data only in accordance with Customer’s documented instructions and as described and subject to the limitations provided below (a) to provide Customer the Online Services in accordance with Customer’s documented instructions, and (b) for business operations associated with providing the Online Services to Customer. As between the parties, Customer retains all right, title and interest in and to Customer Data. 21Vianet acquires no rights in Customer Data, other than the rights Customer grants to 21Vianet in this section. This paragraph does not affect 21Vianet’s rights in software or services 21Vianet licenses to Customer.

**Processing to Provide Customer the Online Services**

For purposes of this DPA, “to provide” an Online Service consists of:

* Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences;
* Troubleshooting (preventing, detecting, and repairing problems); and
* Keeping Online Services up to date and performant, and enhancing user productivity, reliability, efficacy, quality, and security.

Providing Online Services is conducted in view of security obligations under the Data Protection Requirements.

When providing Online Services, 21Vianet will not use or otherwise process Customer Data or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer’s documented instructions.

**Processing for Business Operations associated with Providing the Online Services**

For purposes of this DPA, “business operations” means the processing operations authorized by customer in this section.

Customer authorizes 21Vianet:

1. to create aggregated statistical, non-personal data from data containing pseudonymized identifiers (such as usage logs containing unique, pseudonymized identifiers); and
2. to calculate statistics related to Customer Data

in each case without accessing or analyzing the content of Customer Data and limited to achieving the purposes below, each as incident to providing the Online Services to Customer.

Those purposes are:

* billing and account management;
* compensation such as calculating employee commissions and partner incentives;
* internal reporting and business modeling, such as forecasting, revenue, capacity planning, and product strategy; and
* financial reporting.

When processing for business operations, 21Vianet will apply principles of data minimization and will not use or otherwise process Customer Data or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) any other purpose, other than for the purposes set out in this section. In addition, as with all processing under this DPA, processing for business operations remains subject to 21Vianet’s confidentiality obligations and commitments under Disclosure of Processed Data.

## **Disclosure of Processed Data**

21Vianet will not disclose or provide access to any Processed Data except: (1) as Customer directs; (2) as described in this DPA; or (3) as required by law. For purposes of this section, “Processed Data” means: (a) Customer Data; (b) Personal Data; and (c) any other data processed by 21Vianet in connection with the Online Service that is Customer’s confidential information under 21Vianet Customer Agreement. All processing of Processed Data is subject to 21Vianet’s obligation of confidentiality under the 21Vianet Customer Agreement.

21Vianet will not disclose or provide access to any Processed Data to law enforcement unless required and permitted by applicable laws. If law enforcement contacts 21Vianet with a demand for Processed Data, 21Vianet will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose or provide access to any Processed Data to law enforcement, 21Vianet will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third-party request for Processed Data, 21Vianet will promptly notify Customer unless prohibited by law. 21Vianet will reject the request unless required and permitted by law to comply. If the request is valid, 21Vianet will attempt to redirect the third party to request the data directly from Customer.

21Vianet will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Processed Data; (b) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed Data if 21Vianet is aware that the data is to be used for purposes other than those stated in the third party’s request.

In support of the above, 21Vianet may provide Customer’s basic contact information to the third party.

## **Processing of Personal Data**

All Personal Data processed by 21Vianet in connection with providing the Online Services is obtained as part of either (a) Customer Data, or (b) data generated, derived or collected by 21Vianet, including data sent to 21Vianet as a result of a Customer’s use of service-based capabilities. Personal Data provided to 21Vianet by, or on behalf of, Customer through use of the Online Service is also Customer Data. Pseudonymized identifiers may be included in data processed by 21Vianet in connection with providing the Online Services and are also Personal Data. Any Personal Data pseudonymized, or de-identified but not anonymized, or Personal Data derived from Personal Data is also Personal Data.

The parties also agree to the following terms in this sub-section:

**Roles and Responsibilities of Customer and 21Vianet**

*Processing Subject to the GDPR*

To the extent 21Vianet is a processor or subprocessor of Personal Data subject to the GDPR, the GDPR Terms in [Attachment](#Attachment3) 2 govern that processing and:

Customer and 21Vianet agree that Customer is the controller of Personal Data and 21Vianet is the processor of such data, except (a) when Customer acts as a processor of Personal Data, in which case 21Vianet is a subprocessor; or (b) as stated otherwise in the Online Service Specific terms or this DPA. When 21Vianet acts as the processor or subprocessor of Personal Data, it will process Personal Data only on documented instructions from Customer. Customer agrees that its 21Vianet Customer Agreement (including the DPA Terms and any applicable updates), along with the product documentation and Customer’s use and configuration of features in the Online Services, are Customer’s complete documented instructions to 21Vianet for the processing of Personal Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer’s 21Vianet Customer Agreement. In any instance where the GDPR applies and Customer is a processor, Customer warrants to 21Vianet that Customer’s instructions, including appointment of 21Vianet as a processor or subprocessor, have been authorized by the relevant controller.

To the extent 21Vianet uses or otherwise processes Personal Data subject to the GDPR for business operations associated with providing the Online Services to Customer, 21Vianet will comply with the obligations of an independent data controller under GDPR for such use. 21Vianet is accepting the added responsibilities of a data “controller” under GDPR for such processing to: (a) act consistent with regulatory requirements, to the extent required under GDPR; and (b) provide increased transparency to Customers and confirm 21Vianet’s accountability for such processing. 21Vianet employs safeguards to protect Customer Data and Personal Data in such processing, including those identified in this DPA and those contemplated in Article 6(4) of the GDPR. With respect to processing of Personal Data under this paragraph, 21Vianet makes the commitments set forth in the Additional Safeguards section; for those purposes, (i) any 21Vianet disclosure of Personal Data, as described in the Additional Safeguards section, that has been transferred in connection with business operations is deemed a “Relevant Disclosure” and (ii) the commitments in the Additional Safeguards section apply to such Personal Data.

*Processing Subject to the PIPL*

Customer and 21Vianet agree that Customer is the “handler” of Personal Data under the PIPL (a term under the PIPL that is akin to the controller under the GDPR) and 21Vianet is the “entrusted party” of such data (a term under the PIPL that is akin to the processor under the GDPR), except (a) when Customer acts as an entrusted party of Personal Data, in which case 21Vianet is a Subprocessor; or (b) as stated otherwise in the Online Service Specific terms or this DPA. When 21Vianet acts as the entrusted party or a Subprocessor of Personal Data, it will process Personal Data only on documented instructions from Customer. Customer agrees that its 21Vianet Customer Agreement (including the DPA Terms and any applicable updates), along with the product documentation and Customer’s use and configuration of features in the Online Services, are Customer’s complete documented instructions to 21Vianet for the processing of Personal Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer’s 21Vianet Customer Agreement. In any instance where the PIPL applies and Customer is an entrusted party, Customer warrants to 21Vianet that Customer’s instructions, including appointment of 21Vianet as an entrusted party or a Subprocessor, have been authorized by the relevant “handler”.

To the extent 21Vianet uses or otherwise processes Personal Data subject to the PIPL for business operations associated with providing the Online Services to Customer or for the purpose of administering and performing the 21Vianet Customer Agreement, and where 21Vianet acts as an independent “handler”, 21Vianet will comply with the obligations of an independent “handler” of Personal Data under the PIPL for such use. 21Vianet is accepting the added responsibilities of a data “handler” under the PIPL for such processing to: (a) act consistent with regulatory requirements, to the extent required under the PIPL; and (b) provide increased transparency to Customers and confirm 21Vianet’s accountability for such processing. 21Vianet employs safeguards to protect Customer Data and Personal Data in processing, including those identified in this DPA and those contemplated under the PIPL.

To the extent 21Vianet uses or otherwise processes Personal Data for the purpose of administering and performing the 21Vianet Customer Agreement, as between Customer and 21Vianet, Customer is responsible to obtain all required consents (or otherwise rely on any other applicable legal basis) from the related data subjects under the PIPL for providing their Personal Data to 21Vianet which may transfer such Personal Data to third parties outside China for above mentioned purpose. To the extent required under applicable law, 21Vianet will follow appropriate requirements for cross-border data transfer.

**Processing Details**

The parties acknowledge and agree that:

* **Subject Matter.** The subject-matter of the processing is limited to Personal Data within the scope of the section of this DPA entitled “Nature of Data Processing; Ownership” above, the GDPR and the PIPL.
* **Duration of the Processing.** The duration of the processing shall be in accordance with Customer instructions and the terms of the DPA.
* **Nature and Purpose of the Processing.** The nature and purpose of the processing shall be to provide the Online Service pursuant to Customer’s 21Vianet Customer Agreement and for business operations associated with providing the Online Service to Customer (as further described in the section of this DPA entitled “Nature of Data Processing; Ownership” above).
* **Categories of Data.** The types of Personal Data processed by 21Vianet when providing the Online Service include: (i) Personal Data that Customer elects to include in Customer Data; and (ii) those are as defined in Article 4 of PIPL or expressly identified in Article 4 of the GDPR (as the case may be) that may be generated, derived or collected by 21Vianet, including data sent to 21Vianet as a result of a Customer’s use of service-based capabilities. The types of Personal Data that Customer elects to include in Customer Data may be any categories of Personal Data identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of Personal Data set forth in Appendix B.
* **Data Subjects.** The categories of data subjects are Customer’s representatives and end users, such as employees, contractors, collaborators, and customers, and may include any other categories of data subjects as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of data subjects set forth in Appendix B.

**Data Subject Rights; Assistance with Requests**

21Vianet will make available to Customer, in a manner consistent with the functionality of the Online Service and 21Vianet’s role as a processor of Personal Data of data subjects, the ability to fulfill data subject requests to exercise their rights under the GDPR or PIPL, as the case may be. If 21Vianet receives a request from Customer’s data subject to exercise one or more of its rights under the GDPR or PIPL in connection with an Online Service for which 21Vianet is a data processor or subprocessor, 21Vianet will redirect the data subject to make its request directly to Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Online Service. 21Vianet shall comply with reasonable requests by Customer to assist with Customer’s response to such a data subject request.

**Records of Processing Activities**

To the extent the GDPR or the PIPL requires 21Vianet to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information to 21Vianet and keep it accurate and up-to-date. 21Vianet may make any such information available to a supervisory authority if required by the GDPR or the PIPL, subject to applicable law.

## **Data Security**

**Security Practices and Policies**

21Vianet will implement and maintain appropriate technical and organizational measures to protect Customer Data and Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Those measures shall be set forth in a 21Vianet Security Policy. 21Vianet will make that policy available to Customer, along with other information reasonably requested by Customer regarding 21Vianet security practices and policies.

In addition, those measures shall comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 27018. A description of the security controls for these requirements is available to Customers. Each Core Online Service implements and maintains the security measures set forth in Appendix A for the protection of Customer Data.

21Vianet may add industry or government standards at any time. 21Vianet will not eliminate ISO 27001, ISO 27002, ISO 27018, unless it is no longer used in the industry and it is replaced with a successor (if any).

**Data Encryption**

Customer Data (including any Personal Data therein) in transit over public networks between Customer and 21Vianet, or between 21Vianet data centers, is encrypted by default.

21Vianet also encrypts Customer Data stored at rest in Online Services. In the case of Online Services on which Customer or a third-party acting on Customer’s behalf may build applications (e.g., certain Azure Services), encryption of data stored in such applications may be employed at the discretion of Customer, using either capabilities provided by 21Vianet or obtained by Customer from third parties.

**Data Access**

21Vianet employs least privilege access mechanisms to control access to Customer Data (including any Personal Data therein). Rose-based access controls are employed to ensure that access to Customer Data required for service operations is for an appropriate purpose and approved with management oversight. For Core Online Services, 21Vianet maintains Access Control mechanisms described in the table entitled “Security Measures” in Appendix A; and there is no standing access by 21Vianet personnel to Customer Data and any required access is for a limited time.

**Customer Responsibilities**

Customer is solely responsible for making an independent determination as to whether the technical and organizational measures for an Online Service meet Customer’s requirements, including any of its security obligations under applicable Data Protection Requirements. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Personal Data as well as the risks to individuals) the security practices and policies implemented and maintained by 21Vianet provide a level of security appropriate to the risk with respect to its Personal Data. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls (such as devices enrolled with Microsoft Intune or within a Microsoft Azure customer’s virtual machine or application).

**Auditing Compliance**

21Vianet will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data and Personal Data, as follows:

* Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually.
* Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
* Each audit will be performed by qualified, independent, third-party security auditors at 21Vianet’s selection and expense.

Each audit will result in the generation of an audit report (“21Vianet Audit Report”). If Customer requests, 21Vianet will provide Customer with each 21Vianet Audit Report. The 21Vianet Audit Report will be subject to non-disclosure and distribution limitations of 21Vianet and the auditor.

If the 2021 Standard Contractual Clauses apply, then this section is in addition to Clause 8.9 of the 2021 Standard Contractual Clauses. Nothing in this section of the DPA varies or modifies the 2021 Standard Contractual Clauses or the GDPR Terms or affects any supervisory authority’s or data subject’s rights under the 2021 Standard Contractual Clauses or Data Protection Requirements.

## **Security Incident Notification**

If 21Vianet becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by 21Vianet (each a “Security Incident”), 21Vianet will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer’s administrators by any means 21Vianet selects, including via email. It is Customer’s sole responsibility to ensure Customer’s administrators maintain accurate contact information on each applicable Online Services portal. Customer is solely responsible for complying with its obligations under incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident.

21Vianet shall make reasonable efforts to assist Customer in fulfilling Customer’s obligation under GDPR Article 33, the PIPL or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

21Vianet’s notification of or response to a Security Incident under this section is not an acknowledgement by 21Vianet of any fault or liability with respect to the Security Incident.

Customer must notify 21Vianet promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

## **Data** **Location**

21Vianet will store Customer Data only in China.

21Vianet does not control or limit the regions from which Customer or Customer’s end users may access or move Customer Data. If a Customer transfers any of its Customer Data (including the Personal Data contained in such Customer Data) by allowing such Customer Data to be accessed by any person outside China or move such Customer Data out of China, Customer shall comply with all requirements under the applicable Data Protection Requirements, including China Laws and Regulations.

## **Data Retention and Deletion**

At all times during the term of Customer’s subscription, Customer will have the ability to access, extract and delete Customer Data stored in each Online Service.

Except for free trials, 21Vianet will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of Customer’s subscription so that Customer may extract the data. After the 90-day retention period ends, 21Vianet will disable Customer’s account and delete the Customer Data and Personal Data stored in Online Services within an additional 90 days, unless authorized under this DPA, to retain such data.

The Online Service may not support retention or extraction of software provided by Customer. 21Vianet has no liability for the deletion of Customer Data or Personal Data as described in this section.

## **Processor Confidentiality Commitment**

21Vianet will ensure that its personnel engaged in the processing of Customer Data and Personal Data (i) will process such data only on instructions from Customer or as described in this DPA, and (ii) will be obligated to maintain the confidentiality and security of such data even after their engagement ends. 21Vianet shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to Customer Data and Personal Data in accordance with applicable Data Protection Requirements and industry standards.

## **Notice and Controls on use of Subprocessors**

21Vianet may hire Subprocessors to provide certain limited or ancillary services on its behalf. In limited circumstances, when it is necessary to troubleshoot and improve customer support incidents or solve technical problems, 21Vianet may authorize a Subprocessor located outside the territory of China to access the Customer Data according to applicable laws and regulations. 21Vianet will supervise such access and terminate such access when the problem is resolved in accordance with applicable laws and regulations. Customer consents to the engagement of these third parties and 21Vianet Affiliates as Subprocessors. **The above authorizations will constitute Customer’s prior written consent to the subcontracting by 21Vianet of the processing of Customer Data and Personal Data if such consent is required under the Standard Contractual Clauses, the GDPR Terms or the PIPL.**

21Vianet is responsible for its Subprocessors’ compliance with 21Vianet’s obligations in this DPA. 21Vianet makes available information about Subprocessors on a 21Vianet website. When engaging any Subprocessor, 21Vianet will ensure via a written contract that the Subprocessor may access and use Customer Data or Personal Data only to deliver the services 21Vianet has retained them to provide and is prohibited from using Customer Data or Personal Data for any other purpose. 21Vianet will ensure that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required of 21Vianet by the DPA, including the limitations on disclosure of Processed Data. 21Vianet agrees to oversee the Subprocessors to ensure that these contractual obligations are met.

From time to time, 21Vianet may engage new Subprocessors. 21Vianet will give Customer notice and, as applicable, update the website and provide Customer with a mechanism to obtain notice of that update) of any new Subprocessor at least 14-days in advance of providing that Subprocessor with access to Customer Data or Personal Data. However, with respect to Core Online Services, 21Vianet will give Customer notice and, as applicable, update the website and provide Customer with a mechanism to obtain notice of that update) of any new Subprocessor at least 6-months in advance of providing that Subprocessor with access to Customer Data. If 21Vianet engages a new Subprocessor for a new Online Service that processes Customer Data or Personal Data, 21Vianet will give Customer notice prior to availability of that Online Service.

If Customer does not approve of a new Subprocessor, then Customer may terminate any subscription for the affected Online Service without penalty by providing, before the end of the relevant notice period, written notice of termination that includes an explanation of the grounds for non-approval. If the affected Online Service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, 21Vianet will remove payment obligations for any subscriptions for the terminated Online Service from subsequent invoices to Customer or its reseller.

## **Sensitive Personal Data**

“Sensitive Personal Data”, also known as “Sensitive Personal Information”, which will have the meaning set forth in Article 28 of the PIPL and, if applicable, equivalent terms in other Data Protection Requirements. For clarify, Sensitive Personal Data may include, without limitation the “Biometric Data” as set forth in Article 4 of the GDPR and, if applicable, equivalent terms in other Data Protection Requirements. If Customer uses an Online Service to process Sensitive Personal Data, Customer is responsible for: (i) providing notice to data subjects, including with respect to necessity of such processing and the potential impact on their interest; (ii) obtaining separate consent from data subjects, if Customer relies on consent as the lawful basis to process Sensitive Personal Data; and (iii) taking necessary measures to protect the Sensitive Personal Data as appropriate and required under applicable Data Protection Requirements. 21Vianet will process that Sensitive Personal Data following Customer’s documented instructions (as described in the “Roles and Responsibilities of Customer and 21Vianet” section above) and protect that Sensitive Personal Data in accordance with the data security and protection terms under this DPA.

## **How to Contact 21Vianet**

If Customer believes that 21Vianet is not adhering to its privacy or security commitments, Customer may contact customer support via <https://www.azure.cn/zh-cn/support/contact/> or mail to 21Vianet. 21Vianet’s mailing address is:

**21Vianet Cloud Compliance**

Shanghai Blue Cloud Technology Co., Ltd. (“21Vianet”)

12-13F, Building 6, No.6 Jiuxianqiao Road, Beijing Electronics Zone, Chaoyang District, Beijing 100015, China

# **Appendix A – Security Measures**

21Vianet has implemented and will maintain for Customer Data in the Core Online Services the following security measures, which in conjunction with the security commitments in this DPA (including the GDPR Terms), are 21Vianet’s only responsibility with respect to the security of that data.

| Domain | Practices |
| --- | --- |
| Organization of Information Security | **Security Ownership**. 21Vianet has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.  **Security Roles and Responsibilities**. 21Vianet personnel with access to Customer Data are subject to confidentiality obligations.  **Risk Management Program**. 21Vianet performed a risk assessment before processing the Customer Data or launching the Online Services service.  21Vianet retains its security documents pursuant to its retention requirements after they are no longer in effect. |
| Asset Management | **Asset Inventory**. 21Vianet maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to 21Vianet personnel authorized in writing to have such access.  **Asset Handling**  - 21Vianet classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted.  - 21Vianet imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data.   * 21Vianet personnel must obtain 21Vianet authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside 21Vianet’s facilities. |
| Human Resources Security | **Security Training**. 21Vianet informs its personnel about relevant security procedures and their respective roles. 21Vianet also informs its personnel of possible consequences of breaching the security rules and procedures. 21Vianet will only use anonymous data in training. |
| Physical and Environmental Security | **Physical Access to Facilities**. 21Vianet limits access to facilities where information systems that process Customer Data are located to identified authorized individuals.  **Physical Access to Components**. 21Vianet maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Customer Data they contain.  **Protection from Disruptions**. 21Vianet uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.  **Component Disposal**. 21Vianet uses industry standard processes to delete Customer Data when it is no longer needed. |
| Communications and Operations Management | **Operational Policy**. 21Vianet maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data.  **Data Recovery Procedures**  - On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), 21Vianet maintains multiple copies of Customer Data from which Customer Data can be recovered.  - 21Vianet stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.  - 21Vianet has specific procedures in place governing access to copies of Customer Data.  - 21Vianet reviews data recovery procedures at least every twelve months.  - 21Vianet logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.  **Malicious Software**. 21Vianet has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks.  **Data Beyond Boundaries**  - 21Vianet encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks.  - 21Vianet restricts access to Customer Data in media leaving its facilities.  **Event Logging**. 21Vianet logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity. |
| Access Control | **Access Policy**. 21Vianet maintains a record of security privileges of individuals having access to Customer Data.  **Access Authorization**  - 21Vianet maintains and updates a record of personnel authorized to access 21Vianet systems that contain Customer Data.  - 21Vianet deactivates authentication credentials that have not been used for a period of time not to exceed six months.  - 21Vianet identifies those personnel who may grant, alter or cancel authorized access to data and resources.  - 21Vianet ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/log-ins.  **Least Privilege**  - Technical support personnel are only permitted to have access to Customer Data when needed.  - 21Vianet restricts access to Customer Data to only those individuals who require such access to perform their job function.  **Integrity and Confidentiality**  - 21Vianet instructs 21Vianet personnel to disable administrative sessions when leaving premises 21Vianet controls or when computers are otherwise left unattended.  - 21Vianet stores passwords in a way that makes them unintelligible while they are in force.  **Authentication**  - 21Vianet uses industry standard practices to identify and authenticate users who attempt to access information systems.  - Where authentication mechanisms are based on passwords, 21Vianet requires that the passwords are renewed regularly.  - Where authentication mechanisms are based on passwords, 21Vianet requires the password to be at least eight characters long.  - 21Vianet ensures that de-activated or expired identifiers are not granted to other individuals.  - 21Vianet monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password.  - 21Vianet maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.  - 21Vianet uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.  **Network Design**. 21Vianet has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access. |
| Information Security Incident Management | **Incident Response Process**  - 21Vianet maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.  - For each security breach that is a Security Incident, notification by 21Vianet (as described in the “Security Incident Notification” section above) will be made without undue delay and, in any event, within 72 hours.  - 21Vianet tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time.  **Service Monitoring**. 21Vianet security personnel verify logs at least every six months to propose remediation efforts if necessary. |
| Business Continuity Management | - 21Vianet maintains emergency and contingency plans for the facilities in which 21Vianet information systems that process Customer Data are located.  - 21Vianet’s redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original or last-replicated state from before the time it was lost or destroyed. |

# **Appendix B – Data Subjects and Categories of Personal Data**

**Data subjects**: Data subjects include the Customer’s representatives and end-users including employees, contractors, collaborators, and customers of the Customer. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the Online Services provided by 21Vianet. 21Vianet acknowledges that, depending on Customer’s use of the Online Service, Customer may elect to include personal data from any of the following types of data subjects in the personal data:

* Employees, contractors and temporary workers (current, former, prospective) of Customer;
* Dependents of the above;
* Customer's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
* Users (e.g., customers, clients, patients, visitors, etc.) and other data subjects that are users of Customer's services;
* Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the Customer and/or use communication tools such as apps and websites provided by the Customer;
* Stakeholders or individuals who passively interact with the Customer (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the Customer);
* Minors; or
* Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).

**Categories of data**: The personal data transferred that is included in e-mail, documents and other data in an electronic form in the context of the Online Services. 21Vianet acknowledges that, depending on Customer’s use of the Online Service, Customer may elect to include personal data from any of the following categories in the personal data:

* Basic personal data (for example place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;
* Authentication data (for example user name, password or PIN code, security question, audit trail);
* Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
* Unique identification numbers and signatures (for example social security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
* Pseudonymous identifiers;
* Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
* Commercial Information (for example history of purchases, special offers, subscription information, payment history);
* Biometric Information (for example DNA, fingerprints and iris scans);
* Location data (for example, cell ID, geo-location network data, location by start call/end of the call, location data derived from use of wifi access points);
* Photos, video and audio;
* Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);
* Device identification (for example IMEI-number, SIM card number, MAC address);
* Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);
* HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location and organizations);
* Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
* Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);
* Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;
* Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person’s sex life or sexual orientation, or data relating to criminal convictions or offences) or the similar category of Sensitive Personal Data under the PIPL; or
* Any other personal data identified in Article 4 of the GDPR or Article 4 of the PIPL.

# **Appendix C - Additional Safeguards Addendum**

By this Additional Safeguards Addendum to the DPA (this “Addendum”), Shanghai Blue Cloud Technology Co., Ltd. (“21Vianet”) provides additional safeguards to Customer for the processing of personal data, within the scope of the GDPR, by 21Vianet on behalf of Customer and additional redress to the data subjects to whom that personal data relates.

This Addendum supplements and is made part of, the DPA.

**1. Challenges to Orders.** In the event 21Vianet receives an order from any third party for compelled disclosure of any personal data processed under this DPA, 21Vianet shall:

**a.** use every reasonable effort to redirect the third party to request data directly from Customer;

**b.** promptly notify Customer, unless prohibited under the law applicable to the requesting third party and/or 21Vianet, and, if prohibited from notifying Customer, use all lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible; and

**c.** use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the law of the European Union or applicable Member State law.

If, after the steps described in a. through c. above, 21Vianet remains compelled to disclose personal data, 21Vianet will disclose only the minimum amount of that data necessary to satisfy the order for compelled disclosure.

For purpose of this section, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

**2. Indemnification of Data Subjects.** Subject to Sections 3 and 4, 21Vianet shall indemnify a data subject for any material or non-material damage to the data subject caused by 21Vianet’s disclosure of personal data of the data subject that has been transferred in response to an order from a non-EU/EEA government body or law enforcement agency (a “Relevant Disclosure”). Notwithstanding the foregoing, 21Vianet shall have no obligation to indemnify the data subject under this Section 2 to the extent the data subject has already received compensation for the same damage, whether from 21Vianet or otherwise.

**3. Conditions of Indemnification.** Indemnification under Section 2 is conditional upon the data subject establishing, to 21Vianet’s reasonable satisfaction, that:

**a.** 21Vianet engaged in a Relevant Disclosure;

**b.** the Relevant Disclosure was the basis of an official proceeding by the non-EU/EEA government body or law enforcement agency against the data subject; and

**c.** the Relevant Disclosure directly caused the data subject to suffer material or non-material damage.

The data subject bears the burden of proof with respect to conditions a. though c.

Notwithstanding the foregoing, 21Vianet shall have no obligation to indemnify the data subject under Section 2 if 21Vianet establishes that the Relevant Disclosure did not violate its obligations under Chapter V of the GDPR.

**4. Scope of Damages.** Indemnification under Section 2 is limited to material and non‑material damages as provided in the GDPR and excludes consequential damages and all other damages not resulting from 21Vianet’s infringement of the GDPR.

**5. Exercise of Rights.** Rights granted to data subjects under this Addendum may be enforced by the data subject against 21Vianet irrespective of any restriction in Clauses 3 of the 2021 Standard Contractual Clauses. The data subject may only bring a claim under this Addendum on an individual basis, and not part of a class, collective, group or representative action. Rights granted to data subjects under this Addendum are personal to the data subject and may not be assigned.

**6. Notice of Change.** 21Vianet agrees and warrants that it has no reason to believe that the legislation applicable to it or its sub-processors, including in any country to which personal data is transferred either by itself or through a sub-processor, prevents it from fulfilling the instructions received from the Customer and its obligations under this Addendum or the 2021 Standard Contractual Clauses and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by this Addendum or the 2021 Standard Contractual Clauses, it will promptly notify the change to Customer as soon as it is aware, in which case Customer is entitled to suspend the transfer of data and/or terminate the contract.

# **Attachment 1 –** **The 2021 Standard Contractual Clauses (Controller to Processors)**

Execution of 21Vianet Customer Agreement by Customer includes execution of this Attachment 1, which is countersigned by 21Vianet.

For the purposes of Article 46 of the GDPR for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, Customer (as data exporter) and 21Vianet (as data importer, whose signature appears below) have agreed on the following Clauses in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Annex I.B.

* 1. **Purpose and scope**
     + 1. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 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 (General Data Protection Regulation) for the transfer of data to a third country.
       2. The Parties:
          1. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter ‘entity/ies’) transferring the personal data, as listed in Annex I.A (hereinafter each ‘data exporter’), and
          2. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each ‘data importer’)

have agreed to these standard contractual clauses (hereinafter: ‘Clauses’).

* + - 1. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
      2. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.
  1. **Effect and invariability of the Clauses**
     + 1. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
       2. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.
  2. **Third-party beneficiaries**
     + 1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
          1. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
          2. Clause 8.1(b), 8.9(a), (c), (d) and (e);
          3. Clause 9(a), (c), (d) and (e);
          4. Clause 12(a), (d) and (f);
          5. Clause 13;
          6. Clause 15.1(c), (d) and (e);
          7. Clause 16(e);
          8. Clause 18(a) and (b).
       2. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.
  3. **Interpretation**
     + 1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
       2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
       3. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.
  4. **Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

* 1. **Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

* 1. **Docking clause**
     + 1. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix 1 and signing Annex I.A.
       2. Once it has completed the Appendix 1 and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
       3. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

1. **– OBLIGATIONS OF THE PARTIES**
   1. **Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

* + 1. Instructions
       1. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
       2. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.
    2. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

* + 1. Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix 1 as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix 1 to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

* + 1. Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

* + 1. Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

* + 1. Security of processing
       1. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). 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 purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
       2. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
       3. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all 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.
       4. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.
    2. Sensitive data

Where the transfer 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 (hereinafter ‘sensitive data’), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

* + 1. Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

* + - 1. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
      2. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
      3. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
      4. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

* + 1. Documentation and compliance
       1. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
       2. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
       3. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
       4. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
       5. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.
  1. **Use of sub-processors**
     + 1. The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least six months in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s).  Additionally, the data importer shall specifically inform the controller of any new sub-processor at least 30 days in advance of providing that sub-processor with access to Personal Data other than that which is contained in Customer Data, as such terms are defined in the Data Protection Addendum at https://www.21vbluecloud.com/ostpt/. The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.  Information under this Clause shall be provided in accordance with the terms of the Data Protection Addendum.
       2. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
       3. The data importer shall provide, at the data exporter’s request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
       4. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor’s obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
       5. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.
  2. **Data subject rights**
     + 1. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
       2. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects’ requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
       3. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.
  3. **Redress**
     + 1. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
       2. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
       3. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
          1. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
          2. refer the dispute to the competent courts within the meaning of Clause 18.
       4. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
       5. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
       6. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.
  4. **Liability**
     + 1. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
       2. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
       3. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
       4. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.
       5. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
       6. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
       7. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.
  5. **Supervision**
     + 1. The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
       2. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

1. **– LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**
   1. **Local laws and practices affecting compliance with the Clauses**
      * 1. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
        2. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
           1. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
           2. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
           3. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
        3. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
        4. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
        5. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
        6. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.
   2. **Obligations of the data importer in case of access by public authorities**
      1. Notification
         1. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
            1. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
            2. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
         2. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
         3. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
         4. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
         5. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.
      2. Review of legality and data minimisation
         1. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
         2. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
         3. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.
2. **– FINAL PROVISIONS**
   1. **Non-compliance with the Clauses and termination**
      * 1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
        2. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
        3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
           1. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
           2. the data importer is in substantial or persistent breach of these Clauses; or
           3. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

* + - 1. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
      2. (Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.
  1. **Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Member State in which the data exporter is established.

* 1. **Choice of forum and jurisdiction**
     + 1. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
       2. The Parties agree that those shall be the courts in the Member State in which the data exporter is established.
       3. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
       4. The Parties agree to submit themselves to the jurisdiction of such courts.

1. **LIST OF PARTIES**

**Data exporter(s):**

Customer is the data exporter. The data exporter is a user of Online Services as defined in the Data Protection Addendum between the data exporter and the data importer (“DPA”) and the 21Vianet Online Services Terms (“OST”).   In this Annex I and in Annex II, all capitalised terms used without definition have the meanings ascribed to them in the DPA.

Activities relevant to the data transferred under these Clauses:

Data transfers are needed in order to successfully and efficiently provide 21Vianet’s Online Services to our customers and manage the processing and security of personal data.

21Vianet will use and otherwise process Customer Data and Personal Data only as described and subject to the limitations provided in the DPA and OST to provide a user of the Online Services provided under the DPA (a “Customer”) the Online Services in accordance with Customer’s documented instructions, and (b) for business operations associated with providing Online Services to Customer.

|  |  |  |
| --- | --- | --- |
|  |  |  |

**Data importer(s):**

Name:  Shanghai Blue Cloud Technology Co., Ltd. (“21Vianet”)

Address:

12-13F, Building 6, No.6 Jiuxianqiao Road, Beijing Electronics Zone, Chaoyang District Beijing 100015, China

Contact person’s name, position and contact details:

Shanghai Blue Cloud Technology Co., Ltd.

Attn: Yuyan Liu, Senior Manager of Risk Management

12-13F, Building 6, No.6 Jiuxianqiao Road, Beijing Electronics Zone, Chaoyang District

Beijing 100015, China

Activities relevant to the data transferred under these Clauses:

Data transfers are needed in order to successfully and efficiently provide 21Vianet to our customers and manage the processing and security of personal data.

21Vianet will use and otherwise process Customer Data and Personal Data only as described and subject to the limitations provided in the DPA and OST to provide a user of the Online Services provided under the DPA (a “Customer”) the Online Services in accordance with Customer’s documented instructions, and (b) for business operations associated with providing the Online Services to Customer.

1. **DESCRIPTION OF TRANSFER**

*Categories of data subjects whose personal data is transferred*

**Data subjects:**  Data subjects include the data exporter’s representatives and end-users including employees, contractors, collaborators, and customers of the data exporter as detailed in Appendix B to the DPA.

*Categories of personal data transferred*

**Categories of data:**  The personal data transferred that is included in e-mail, documents, and other data in an electronic form in the context of the Online Services.  21Vianet acknowledges that, depending on data exporter’s use of the Online Services, data exporter may elect to include personal data from any of the categories detailed in Appendix B to the DPA.

*Sensitive data transferred (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.*

Data importer has implemented and will maintain the security measures set forth at Annex II.

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

Data may be transferred on a continuous basis.

*Nature of the processing/Purpose(s) of the data transfer and further processing*

Customer Data and Personal Data will be used and otherwise processed only as described and subject to the limitations provided in the DPA (a) to provide data exporter the Online Services in accordance with data exporter’s documented instructions, and (b) for business operations incident to providing the Online Services to data exporter.

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

Except for free trials, Data importer will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of data exporter’s subscription so that data exporter may extract the data. After the 90-day retention period ends, Data importer will disable data exporter’s account and delete the Customer Data and Personal Data stored in Online Services within an additional 90 days, unless Data importer is permitted or required by applicable law, or authorized under this DPA, to retain such data.

The Online Service may not support retention or extraction of software provided by data exporter. Data importer has no liability for the deletion of Customer Data or Personal Data as described in this section.

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

Data importer may hire Subprocessors to provide certain limited or ancillary services on its behalf. Data importer is responsible for its Subprocessors’ compliance with 21Vianet’s obligations in the DPA. Data importer makes available information about Subprocessors on a 21Vianet’s website. When engaging any Subprocessor, Data importer will ensure via a written contract that the Subprocessor may access and use Customer Data or Personal Data only to deliver the services Data importer has retained them to provide and is prohibited from using Customer Data or Personal Data for any other purpose. Data importer will ensure that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required of 21Vianet by the DPA, including the limitations on disclosure of Processed Data. Data importer agrees to oversee the Subprocessors to ensure that these contractual obligations are met.

1. **COMPETENT SUPERVISORY AUTHORITY**

*Identify the competent supervisory authority/ies in accordance with Clause 13*

The competent supervisory authority of the Member State in which the data exporter is established.

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

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 8.6(a) and 10(b):

**Technical and Organisational Measures**

With respect to the processing and security of Customer Data or Personal Data in connection with the Online Services, the data importer has implemented and will maintain security measures as described in Appendix A – Security Measures to the DPA.

Data importer provides the additional safeguards as described in Appendix C - Additional Safeguard Addendum to the DPA for data transferred to it as the data importer.

Data importer will implement and maintain appropriate technical and organisational measures to protect Customer Data and Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Those measures shall be set forth in a 21Vianet Security Policy. Data importer will make that policy available to the data exporter, along with other information reasonably requested by the data exporter regarding 21Vianet security practices and policies.

In addition, those measures shall comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 27018. A description of the security controls for these requirements is available to data exporter.

**SUPPLEMENT FOR SWITZERLAND**

For transfers of Customer Data and Personal Data out of Switzerland to provide the Online Services, which are governed by the 2021 Standard Contractual Clauses, and which are also subject to the Swiss Federal Act on Data Protection (FADP) (in addition to being subject to the GDPR), the 2021 Standard Contractual Clauses shall be amended as follows:

* Clause 4 a.: the terms “personal data” and “data subject” as used in these Clauses shall be interpreted as to encompass the respective definitions in the FADP.
* Clause 13: The competent supervisory authority (to be named in Annex I.C) is the Swiss Federal Data Protection and Information Commissioner (FDPIC) to the extent as the data transfer is governed by the FADP.
* Clause 18 c.: This clause shall be interpreted in such a way that a data subject with habitual residence in Switzerland may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland.

**Signing the Standard Contractual Clauses, Appendix on behalf of the data importer:**

Signature: Johnny Liu

文本

描述已自动生成

Title: President

Shanghai Blue Cloud Technology Co., Ltd. (“21Vianet”)

12-13F, Building 6, No.6 Jiuxianqiao Road, Beijing Electronics Zone, Chaoyang District Beijing 100015, China

# **Attachment 2 – European Union General Data Protection Regulation Terms**

21Vianet makes the commitments in these GDPR Terms, to all customers effective May 25, 2018. These commitments are binding upon 21Vianet with regard to Customer regardless of (1) the version of the OST and DPA that is otherwise applicable to any given Online Services subscription or (2) any other agreement that references this attachment.

For purposes of these GDPR Terms, Customer and 21Vianet agree that Customer is the controller of Personal Data and 21Vianet is the processor of such data, except when Customer acts as a processor of Personal Data, in which case 21Vianet is a subprocessor. These GDPR Terms apply to the processing of Personal Data, within the scope of the GDPR, by 21Vianet on behalf of Customer. These GDPR Terms do not limit or reduce any data protection commitments 21Vianet makes to Customer in the Use Rights or other agreement between 21Vianet and Customer. These GDPR Terms do not apply where 21Vianet is a controller of Personal Data.

**Relevant GDPR Obligations: Articles 28, 32, and 33**

1. 21Vianet shall not engage another processor without prior specific or general written authorisation of Customer. In the case of general written authorisation, 21Vianet shall inform Customer of any intended changes concerning the addition or replacement of other processors, thereby giving Customer the opportunity to object to such changes. (Article 28(2))
2. Processing by 21Vianet shall be governed by these GDPR Terms under European Union (hereafter “Union”) or Member State law and are binding on 21Vianet with regard to Customer. The subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data, the categories of data subjects and the obligations and rights of the Customer are set forth in the Customer’s licensing agreement, including these GDPR Terms. In particular, 21Vianet shall:
3. process the Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which 21Vianet is subject; in such a case, 21Vianet shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
4. ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
5. take all measures required pursuant to Article 32 of the GDPR;
6. respect the conditions referred to in paragraphs 1 and 3 for engaging another processor;
7. taking into account the nature of the processing, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer’s obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;
8. assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to 21Vianet;
9. at the choice of Customer, delete or return all the Personal Data to Customer after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data;
10. make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.

21Vianet shall immediately inform Customer if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. (Article 28(3))

1. Where 21Vianet engages another processor for carrying out specific processing activities on behalf of Customer, the same data protection obligations as set out in these GDPR Terms shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, 21Vianet shall remain fully liable to the Customer for the performance of that other processor's obligations. (Article 28(4))
2. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Customer and 21Vianet shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
3. the pseudonymisation and encryption of Personal Data;
4. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
5. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
6. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. (Article 32(1))
7. In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. (Article 32(2))
8. Customer and 21Vianet shall take steps to ensure that any natural person acting under the authority of Customer or 21Vianet who has access to Personal Data does not process them except on instructions from Customer, unless he or she is required to do so by Union or Member State law. (Article 32(4))
9. 21Vianet shall notify Customer without undue delay after becoming aware of a Personal Data breach. (Article 33(2)). Such notification will include that information a processor must provide to a controller under Article 33(3) to the extent such information is reasonably available to 21Vianet.