21Vianet

21Vianet Online Services Data Protection Addendum

Last updated January 15, 2022

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

**Table of Contents**

[Introduction 3](#_Toc92899346)

[Applicable DPA Terms and Updates 3](#_Toc92899347)

[Electronic Notices 3](#_Toc92899348)

[Prior Versions 3](#_Toc92899349)

[Definitions 4](#_Toc92899350)

[General Terms 5](#_Toc92899351)

[Compliance with Laws 5](#_Toc92899352)

[Data Protection Terms 5](#_Toc92899353)

[Scope 5](#_Toc92899354)

[Nature of Data Processing; Ownership 5](#_Toc92899355)

[Disclosure of Processed Data 6](#_Toc92899356)

[Processing of Personal Data 6](#_Toc92899357)

[Data Security 8](#_Toc92899358)

[Security Incident Notification 8](#_Toc92899359)

[Data Location 9](#_Toc92899360)

[Data Retention and Deletion 9](#_Toc92899361)

[Processor Confidentiality Commitment 9](#_Toc92899362)

[Notice and Controls on use of Subprocessors 9](#_Toc92899363)

[Sensitive Personal Data 10](#_Toc92899364)

[How to Contact 21Vianet 10](#_Toc92899365)

[Appendix A – Security Measures 11](#_Toc92899366)

[Appendix B – Data Subjects and Categories of Personal Data 14](#_Toc92899367)

[Appendix C - Additional Safeguards Addendum 16](#_Toc92899368)

[Attachment 1 – The 2010 Standard Contractual Clauses (Processors) 17](#_Toc92899369)

[Attachment 2 – European Union General Data Protection Regulation Terms 22](#_Toc92899370)

# **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 10 of the 2010 Standard Contractual Clauses in [Attachment](#Attachment1) 1, when the 2010 Standard Contractual Clauses are applicable, the 2010 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 the People’s Republic 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.

“2010 Standard Contractual Clauses” means the standard data protection clauses 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 decision 2010/87/EC, dated 5 February 2010. The 2010 Standard Contractual Clauses are in [Attachment](#Attachment1) 1.

“2021 Standard Contractual Clauses” means the standard data protection clauses (processor-to-processor module) for the transfer of personal data from processors in the EEA 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.

“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. The terms “data importer” and “data exporter” have the meanings given in the 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 security breach notification law 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 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 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
* Ongoing improvement (installing the latest updates and making improvements to user productivity, reliability, efficacy, quality, and security).

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**

For purposes of this DPA, “ business operations” consist of the following, each as associated with providing the Online Services to Customer: (1) billing and account management; (2) compensation (e.g., calculating employee commissions and partner incentives); (3) internal reporting and business modeling (e.g., forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, cybercrime, or cyber-attacks that may affect 21Vianet or 21Vianet Products; (5) improving the core functionality of accessibility, privacy or energy-efficiency; and (6) financial reporting and compliance with legal obligations (subject to the limitations on disclosure of Processed Data outlined below).

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.

## **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 by law. 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 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 processing in connection with its business operations 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 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 equivalent to the controller under the GDPR) and 21Vianet is the processor of such data (as defined under the PIPL), 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 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 a processor, Customer warrants to 21Vianet that Customer’s instructions, including appointment of 21Vianet as a processor 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, as between Customer and 21Vianet, 21Vianet will comply with the obligations of an independent “handler” of Personal Data under the PIPL for such use, and Customer is responsible to obtain all required consents 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 business operations purpose. 21Vianet is accepting the added responsibilities of a data “handler” under the PIPL for processing in connection with its business operations 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.

**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 PIPL or GDPR, 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 PIPL or GDPR 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 the supervisory authority if required by the GDPR or the PIPL.

## **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 2010 Standard Contractual Clauses apply, then this section is in addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the 2010 Standard Contractual Clauses. Nothing in this section of the DPA varies or modifies the 2010 Standard Contractual Clauses or the GDPR Terms or affects any supervisory authority’s or data subject’s rights under the 2010 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 (by updating 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 (by updating 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
* Any other personal data identified in Article 4 of the PIPL or Article 4 of the GDPR.

# **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, 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 or 6 of the 2010 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 data exporter and its obligations under this Addendum, the 2010 Standard Contractual Clauses, 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 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.

**7. Termination.** This Addendum shall automatically terminate if the European Commission, a competent Member State supervisory authority, or an EU or competent Member State court approves a different lawful transfer mechanism that would be applicable to the personal data in the Customer Data, or other Personal Data that is processed under the DPA, (and if such mechanism applies only to some of that data , this Addendum will terminate only with respect to that data) and that does not require the additional safeguards set forth in this Addendum.

# **Attachment 1 –** **The 2010 Standard Contractual Clauses (Processors)**

Execution of the 21Vianet Customer Agreement by Customer includes execution of this Attachment 1, which is countersigned by 21Vianet. This Attachment 1 is in addition to the 2021 Standard Contractual Clauses if 21Vianet is required to execute under the GDPR. In the case of any inconsistency between this Attachment 1 and the 2021 Standard Contractual Clauses (if executed by 21Vianet), the inconsistency shall be resolved so as to provide an adequate level of data protection for the Customer Data and Personal Data under applicable law. To opt out of the “Standard Contractual Clauses”, Customer must send the following information to 21Vianet in a written notice (under terms of the 21Vianet Customer Agreement):

* the full legal name of the Customer and any Affiliate that is opting out;
* if Customer has multiple 21Vianet Customer Agreements, the 21Vianet Customer Agreement to which the Opt Out applies; and
* a statement that Customer (or Affiliate) opts out of the Standard Contractual Clauses.

In countries where regulatory approval is required for use of the Standard Contractual Clauses, the Standard Contractual Clauses cannot be relied upon under European Commission 2010/87/EU (of February 2010) to legitimize export of data from the country, unless Customer has the required regulatory approval.

Beginning May 25, 2018 and thereafter, references to various Articles from the Directive 95/46/EC in the Standard Contractual Clauses below will be treated as references to the relevant and appropriate Articles in the GDPR.

For the purposes of Article 26(2) of Directive 95/46/EC 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), each a “party,” together “the parties,” have agreed on the following Contractual Clauses (the “Clauses” or “Standard Contractual 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 Appendix 1.

**Clause 1: Definitions**

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

**Clause 2: Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 below which forms an integral part of the Clauses.

**Clause 3: Third-party beneficiary clause**

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

**Clause 4: Obligations of the data exporter**

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 below;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

**Clause 5: Obligations of the data importer**

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract 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 the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11; and

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

**Clause 6: Liability**

1. The parties agree that any data subject who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

**Clause 7: Mediation and jurisdiction**

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

**Clause 8: Cooperation with supervisory authorities**

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

**Clause 9: Governing Law.**

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

**Clause 10: Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

**Clause 11: Subprocessing**

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

**Clause 12: Obligation after the termination of personal data processing services**

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**Appendix 1 to the Standard Contractual Clauses**

**Data exporter**: Customer is the data exporter. The data exporter is a user of Online Services as defined in the DPA and OST.

**Data importer:** The data importer is 21Vianet, an operator of Microsoft Azure, Microsoft Dynamics 365, Office 365, and Microsoft Power BI services in China.

**Data subjects**: Data subjects include the data exporter’s representatives and end-users including employees, contractors, collaborators, and customers of the data exporter.

**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 categories in Appendix B to the DPA.

**Processing operations**: The personal data transferred will be subject to the following basic processing activities:

**a. Duration and Object of Data Processing**. The duration of data processing shall be for the term designated under the applicable 21Vianet Customer Agreement between data exporter and the 21Vianet entity to which these Standard Contractual Clauses are annexed (“21Vianet”). The objective of the data processing is the performance of Online Services.

**b. Scope and Purpose of Data Processing**. The scope and purpose of processing personal data is described in the “Processing of Personal Data; GDPR” section of the DPA. The processing may take place in any jurisdiction where data importer or its sub-processors operate such facilities in accordance with the “Security Practices and Policies” section of the DPA.

**c. Customer Data and Personal Data Access**. For the term designated under the applicable 21Vianet Customer Agreement data importer will at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide data exporter with the ability to correct, delete, or block Customer Data and personal data, or (2) make such corrections, deletions, or blockages on its behalf.

**d. Data Exporter’s Instructions**. For Online Services , data importer will only act upon data exporter’s instructions as conveyed by 21Vianet.

**e. Customer Data and Personal Data Deletion or Return**. Upon expiration or termination of data exporter’s use of Online Services, it may extract Customer Data and personal data and data importer will delete Customer Data and personal data, each in accordance with the DPA Terms applicable to the agreement.

**Subcontractors**: In accordance with the DPA, the data importer may hire other companies to provide limited services on data importer’s behalf, such as providing customer support. Any such subcontractors will be permitted to obtain Customer Data and personal data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Customer Data and personal data for any other purpose.

**Appendix 2 to the Standard Contractual Clauses**

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

1. **Personnel**. Data importer’s personnel will not process Customer Data or personal data without authorization. Personnel are obligated to maintain the confidentiality of any such Customer Data and personal data and this obligation continues even after their engagement ends.

2. **Data Privacy Contact.** The data privacy officer of the data importer can be reached at the following address:

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

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

Beijing 100015, China

3. **Technical and Organization Measures.** The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Customer Data and personal data, as defined in the Security Practices and Policies section of the DPA, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows: The technical and organizational measures, internal controls, and information security routines set forth in the Security Practices and Policies section of the DPA are hereby incorporated into this Appendix 2 by this reference and are binding on the data importer as if they were set forth in this Appendix 2 in their entirety.

**Signing the Standard Contractual Clauses, Appendix 1, and Appendix 2 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:

**(a)** 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;

**(b)** ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

**(c)** take all measures required pursuant to Article 32 of the GDPR;

**(d)** respect the conditions referred to in paragraphs 1 and 3 for engaging another processor;

**(e)** 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;

**(f)** 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;

**(g)** 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;

**(h)** 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))

**3.** 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))

**4.** 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:

**(a)** the pseudonymisation and encryption of Personal Data;

**(b)** the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

**(c)** 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

**(d)** 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))

**5.** 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))

**6.** 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))

**7.** 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.