Privacy Statement for Online Services Operated by 21Vianet

Updated: 11/1/2018

Scope

Online services operated by Shanghai Blue Cloud Technology Co., Ltd., a wholly owned subsidiary of Beijing 21Vianet Broadband Data Center Co., Ltd., (“21Vianet, or “we”) include (i) Microsoft Azure; and (ii) Office 365 and Power BI (“Services”). The online services operated by 21Vianet are cloud services based on Microsoft’ s technology but operated and sold by 21Vianet from data centers located in the People’ s Republic of China (excluding Hong Kong and Macau Special Administrative Regions and Taiwan, referred to below as “China”). This Statement applies to the use of those services and any other 21Vianet services that display or link to this Statement. These services are referred to in this Statement collectively as the "Services". For more information about the functionality of particular features, please review the service description or service documentation available on the Azure Developer Center.

The Services may enable you to purchase, subscribe or use other products and services from 21Vianet or third parties with different privacy practices. Your use of other products and services, and any information you provide to a third party is governed by their privacy statements and policies.

Notice to End Users: This Privacy Statement is written for customers and potential customers of the online services operated by 21Vianet (collectively referred to as our "Customers"). All references to "you" or "your" in this privacy statement are to 21Vianet customers, who, in turn, may use the Services to develop and host their own services for their end users. Any information 21Vianet collects or handles in such circumstances is processed by us on behalf of our customer, who controls the collection and use of the information. End users should direct privacy-related requests to the entity providing them with service. If an end user accesses the Services using an email address provided by his or her organization (e.g., employer or school), the owner of the domain associated with the email address may: (i) have control and power of administration over the end user's service account; and (ii) access and process end-user data, including the content of end-user’ s communications and files. The end user's use of the Services may be subject to the organization's policies (if any). End users should submit their privacy-related claims directly to their own organization's administrators. We are only responsible for the customer's privacy-related practices within the scope agreed with the customer.

How We Collect and Use Your Data

Definition of Personal Information

Personal Information refers to all kinds of information recorded via electronic means or otherwise that can be used to identify a particular natural person or to

reflect the particular natural person’ s activities, whether on its own or combined with other information. For the purpose of this Privacy Statement, personal information may include the administrator data of the account administrator you specify in the portal, real-name authentication data, the name, the number of the payment instrument, the billing address in the payment data, the registration data you submit on our website, in our marketing event, or for any survey or questionnaire, as well as the contact and verification information in support data, etc.

Sensitive Personal Information refers to personal information that can easily lead to damage of personal reputation, physical and mental health, or discriminatory treatment, and may endanger the safety of people and property if it is revealed, illegally provided, or abused. For the purpose of this Privacy Statement, personal sensitive information may include administrator data, real-name authentication data, payment data, registration data which includes personal phone number, e-mail address, identification and payment instrument account numbers, security code, transaction record, support data which includes contact and verification information, etc.

We collect and use your data in the following scenarios, which may involve personal information. If we collect your personal information beyond the scope of the following statement, or use your personal information beyond the scope directly or reasonably associated with the stated purpose at the time of collection,

we will inform you again and obtain your express consent before collecting or using your personal information.

Customer Data

Customer Data is all the data, including all text, sound, software or image files that you provide, or are provided on your behalf, to us through your use of the Services. For example, Customer Data includes data that you upload for storage or processing in the Services and applications that you or your end users upload for hosting in the Services. It does not include configuration, technical settings, or support ticket information, or Administrator Data, Real-Name Authentication Data, and Payment Data indicated below.

We only use Customer Data to provide the Services and for purposes compatible with providing the Services. This may include improvement of underlying technology, troubleshooting aimed at preventing, detecting and repairing problems affecting the operation of the Services and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam).

Customer Data will only be stored in data centers located in China. In limited circumstances, when it is necessary to troubleshoot customer support incidents or solve technical problems, 21Vianet may authorize an affiliate, supplier or subcontractor 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.

Administrator Data

Administrator Data is the information about administrators (including account contact and subscription administrators) provided during sign-up, purchase, or administration of the Services, such as name, address, phone number, and e-mail address.

We use Administrator Data to complete the transactions you request, administer your account, improve the Services, and detect and prevent fraud.

We may contact you to provide information about new subscriptions, billing and important updates about the Services, including information about security or other technical issues. We may also contact you regarding third-party inquiries we receive regarding your use of the Services, as described in your customer agreement. You will not be able to unsubscribe from these communications during the reasonable period within or after the Services. Subject to your contact preferences, you may also be contacted, by phone or e-mail, regarding information and offers about other products and services or to request your feedback. You may manage your contact preferences or unsubscribe such communications in your account profile.

Real-Name Authentication Data

We implement real-name management in accordance with laws and regulations. Real-Name Authentication Data refers to your business license, administrator's mobile phone number, or the scanned copy of ID card provided by you during real-name authentication. If you do not provide the above information, you will not be able to complete the real name authentication and may not be able to use the Services.

In order to verify the accuracy and completeness of the Real-Name Authentication Data, we may verify the information provided by you with agencies that legally store your information.

Payment Data

When you make online purchases, you will be asked to provide payment information, which includes your payment instrument number, your name and billing address, and the security code associated with your payment instrument and other financial data ("Payment Data").

We use Payment Data to complete transactions, as well as for the detection and prevention of fraud.

When you use authenticated Payment Data, we will store that data to help you complete future transactions without your having to provide the information again. We do not, however, retain the security code associated with your payment instrument in this manner.

Support Data

Support Data is the information we collect when you submit a support request or run an automated fault detector, including information about hardware and software, and other details related to support incidents, such as contact or verification information, chat session personalization, information about the conditions of the device and application during the period of error and diagnostics, system and registration data regarding software installation and hardware configuration, and error tracking files.

Support services can be provided by phone, email or online chat. With your permission, we may temporarily manipulate your machine through Remote Access (RA). Calls, live chat, or remote access by professional support staff may be recorded and/or monitored. For remote access, you can also view the record after the operation has ended. You can choose to terminate live chat or remote access at any time. We use support data in accordance with this Privacy Statement, and we also use it to resolve your support issues and for training purposes.

After the support experience is over, we may send you a questionnaire about your experience and service content. If you are unwilling to participate in the survey, you may unsubscribe through the footer link in the email or contact the support department through other communication methods provided by 21Vianet to unsubscribe.

How We Use Cookies and Similar Technologies

Some Online Services' websites use "Cookies", which are small text files placed on a device's hard drive by a web server. We may use Cookies and similar technologies such as web beacons for storing users' preferences and settings, to prevent fraud, authenticate users and collect operational information about the Services. In addition to the Cookies we may set when you visit our websites, third parties that provide certain services on our behalf, such as site analytics, may also set certain Cookies on your hard drive when you visit our sites.

You may object or manage Cookies through changing the settings on your browser. However, please note that if you stop using Cookies, you may not enjoy the best service experience, and some of our Services may not function properly.

Local Software

Some features of Online Services may enable or require that you install or run local software (e.g., agents, Azure Stack software, etc.). Such software may collect data from your local environment in order to provide the Services that you have requested. Local agents may also collect telemetry information that will be sent to us (including our affiliates, and domestic or overseas suppliers or subcontractors) for operating and improving the Services. For more information about agents, please consult the relevant service documentation.

How We Store Your Personal Information

Your personal information will be stored in China. If necessary, your personal information may be transferred overseas upon your authorization or in accordance with applicable laws and regulations.

During your use of the Services, we retain the information you provided. After you close your account, in accordance with relevant laws and regulations, we will retain your information, but we will not use or process your information during this period; upon expiry of the aforementioned retention period, we will immediately delete or anonymize your information.

When we terminate a service or operation, we will notify you by e-mail or announcement, and delete or anonymize your relevant personal information upon such termination.

How We Share, Transfer, and Disclose Your Information

We will not disclose or transfer Customer Data, Administrator Data, Real-Name Authentication Data, Payment Data or any other personal information ("your information") to, or share your information with, any third party apart from 21Vianet and its affiliates except as you direct, or as described in your agreement or this Privacy Statement, or pursuant to applicable laws and regulations.

- We contract with other companies within or outside China from time to time to provide technical support or services (such as customer support) on our behalf. We may provide these companies with access to your

information where necessary for their engagement. This information mainly includes various technical information for providing technical support or services, and in rare cases involves your personal information. If it is really necessary to have your personal information accessed by an overseas supplier or subcontractor, our customer support personnel will explain the relevant information to you and obtain your prior consent. These companies are required to maintain the confidentiality of your information and are prohibited from using it for any purpose other than that for which they are engaged by 21Vianet.

- If it is strictly necessary to disclose Customer Data to a third party, we will use commercially reasonable efforts to notify you in advance of the disclosure unless legally prohibited. Should a third party contact us with a complaint about your use of the Services (for example, allegation of infringement by you or your end user), we may ask the third party to contact you directly and may provide your basic contact information to the third party.
- 21Vianet may share Administrator Data or Payment Data with third parties within or outside China for the purpose of fraud prevention or to process payment transactions. Currently, the data of such overseas subcontractors are stored in the US and other countries or regions. The third parties are required to keep your information confidential and are prohibited from using it for other purposes. They are required to take adequate security

measures to ensure that your personal information receives the level of protection no less than that in China.

- The Services enable you to purchase, subscribe to, or use services, software, and contents from companies other than 21Vianet ("Third Party Offerings"). If you choose to purchase, subscribe to, or use a Third Party Offering, we may provide the third party with your Administrator Data or Payment Data to enable the third party to provide its offering to you (and subject to your contact preferences, send you promotional communications). That information and your use of a Third Party Offering will be governed by the privacy statement and policies applicable to the third party.
- We will not substantively respond to data protection and privacy requests from your end users without your prior written instruction, unless required by applicable laws.
- If your personal information has to be transferred due to acquisitions, mergers, reorganizations or similar transactions, we will notify you such situation. The succeeding company that holds your personal information will continue to perform the responsibilities and obligations under this Privacy Statement. If the succeeding company modifies the purpose of using your personal information, it should acquire your explicit consent again with regard to such modification.

- We may not need to obtain your explicit instruction when sharing, transferring or disclosing your personal information under the following circumstances:
    - circumstances directly related to national security and national defense;
    - circumstances directly related to public security, public health and significant public interests;
    - circumstances directly related to criminal investigation, prosecution, trial, execution of a sentence, etc.;
    - for securing significant lawful interests, such as your or other person’ s life, property, etc., but it is difficult to acquire the consent from the personal information subject;
    - where you have already publicly disclosed your personal information; and
    - where we collect your personal information from the information that is lawfully disclosed to the public, such as from legitimate news report or information published by the government.

How We Protect Your Personal Information

We are committed to protecting your personal information. We use a variety of security technologies and procedures to help protect your personal information from unauthorized access, use, or disclosure. For example, we store your personal

information on computer systems located in controlled locations and restrict access to these systems. When storing and transmitting your personal information, we will take appropriate security measures such as encryption.

In the event of personal information security incidents, 21Vianet will promptly notify you via push notifications or announcements in accordance with the requirements of laws and regulations, informing you of the basic circumstances and possible impacts of the security incidents, the measures we have taken or will take, advice for you on self-prevention and mitigation of risks, remedial measures for you, etc.

In the event of a cybersecurity incident, we will follow the emergency response plan for cybersecurity incidents, take appropriate remedial measures, and report to the competent authorities in accordance with relevant laws and regulations.

How You Can Manage Your Personal Information

We provide you with ways to manage your personal information. You can access and manage your administrator data, real-name authentication data, and payment data in the account information of your administrator portal. However, for security and identification considerations or as required by laws and regulations, you may not be able to modify the initial registration information provided at the time of registration, such as real-name authentication data.

If you have other questions or needs for managing personal information, please contact customer support. If you choose to delete your personal information or

change the scope of the authorization, it may result in our failure to provide certain Services for you. For example, deleting payment information or contact details will make it difficult for you to complete payments and receive corresponding Services.

If we decide to respond to your request for deletion, we will also notify the supplier or subcontractor who has obtained your personal information from us and request them to delete your personal information in a timely manner, unless otherwise required by laws and regulations.

To ensure security, we may ask you to verify your identity first in response to your request to manage personal information under this section. We will timely respond to your request above after verifying your identity, and reply or make reasonable explanations to you within 30 days or the time limit stipulated by applicable laws and regulations, or inform you about the external approaches you may choose to resolve the disputes.

Notwithstanding the above, pursuant to applicable laws and regulations, we may not need to respond to your requests under the following circumstances, including but not limited to:

- circumstances directly related to national security and national defense;
- circumstances directly related to public security, public health and significant public interests;

- circumstances directly related to criminal investigation, prosecution, trial, execution of a sentence, etc.;
- where the personal information controller has sufficient evidence showing that the personal information subject has mens rea or abuses his or her rights;
- where responding to the request of the personal information subject will result in serious damage to the legitimate rights and interests of the personal information subject or other individuals and organizations; and
- circumstances involving trade secrets.

Compliance with Law

You acknowledge that under Chinese regulations:

- An Internet information service provider shall not produce, reproduce, publish, or disseminate information that contains the following contents (“Prohibited Contents”). Prohibited Contents are contents that:
    - are against the basic principles determined by the Constitution;
    - impair national security, divulge State secrets, subvert State sovereignty or jeopardizes national unity;
    - damage the reputation and interests of the State;
    - incite ethnic hostility and ethnic discrimination, or jeopardize unity among ethnic groups;

        - damage State religious policies or that advocate religious cults or feudal superstitions;
        - disseminate rumors, disrupt social order or damage social stability;
        - disseminate obscenity, pornography, gambling, violence, homicide and terror, or that incite crime;
        - insult or slander others or that infringe their lawful rights and interests;
        - are otherwise prohibited by laws or administrative regulations.
    - If an Internet information service provider discovers that information distributed on its website falls within the scope of the Prohibited Contents, it shall promptly terminate the distribution, keep relevant records, and report to relevant authorities.

You further agree that:

- If the business you operate by using the Services is subject to permit or approval by relevant governmental authorities, you should obtain such relevant permit or approval, including but not limited to:
    - if your website provides non-operational Internet information services, you should make the filing with relevant governmental authority for the website;
    - if your website provides operational Internet information services, you should obtain an ICP license from relevant governmental authorities for the website.

- If you are an Internet information service provider using the Services, you should keep records of the information provided, time of publishing and the Internet address or domain name, and assist in providing such information when inquired by relevant government authorities in accordance with applicable laws.
- You will provide your real identity and contact information when signing up for the Services and promptly update that information in the Portal if there are any changes to the information. We will use this information to contact you, as detailed in this Privacy Statement. You guarantee that the information you provide is true, complete and valid; otherwise, you will bear all the consequences.

Trial Period

Service trials are provided to examine Services prior to purchase. At the end of the trial period, 21Vianet can temporarily retain the information it collects during your service trial to improve your customer experience when you decide to purchase the Services in the future. However, your information may be removed from the Services at any time after the service trial period ends.

Preview Releases

Preview version, beta version or other pre-release services ("Previews") are optional evaluation versions of the Services offered by 21Vianet to obtain

customer feedback prior to general release. This section describes the different or additional terms specific to Previews:

- Security: We will do our best to provide security measures for your data in the Previews, but these security measures may differ from the present security measures in typical Services.

Protection of Minors

If you are a minor under the age of 18, please be sure to ask your guardian to read the Privacy Statement carefully, and please use our Services or provide your information to us under the condition that you have obtained the consent of your guardian.

Changes to this Privacy Statement

We will update our Privacy Statement from time to time to reflect requirements of applicable laws and regulations, customer feedbacks and changes in our Services. When we post changes to the Statement, we will revise the "last updated" date at the top of the Statement. If there are substantial changes to the Statement or in how 21Vianet will use your information, we will notify you either by posting a notice or by directly sending you a notification about such changes before they take effect. We encourage you to periodically review the Privacy Statement for the products and services you use to learn about how 21Vianet protects your information.

How to Contact Us

21Vianet welcomes your comments. If you believe that 21Vianet is not adhering to its privacy or security commitments, or you need more help from us, please contact us through Customer Support. We have a personal information protection officer. Our mailing address is:

12-14F, Building 6, No.6, Jiuxianqiao Road, Beijing Electronics Zone, Chaoyang District, Beijing, 100015

Shanghai Blue Cloud Technology Co., Ltd, a wholly owned subsidiary of Beijing 21Vianet Broadband Data Center Co., Ltd.

We will respond to you within 30 days after the verification of your identity.