VDMA China

China Office

Cloud and Cloud Applications in China

Date: 06/2021

Summary

1. Introduction

Using cloud services is part of the daily business operations for foreign invested companies in China. In the following, basic information regarding cloud and cloud applications in China will be explained. The focus will be on the following questions:

- Can a company build its own cloud, or should it use the services from a Chinese cloud provider?
- Should the use of clouds in China be registered in China?
- Are there any restrictions for cloud services in China?
- Can the cloud be visited from Germany or other countries in the world?
- What are the major cloud providers in China?
- What else should companies pay attention to regarding the use of clouds?

2. Summary of the conclusions

- Foreign invested companies (such as subsidiaries of German companies) in China may use public cloud services (like Alibaba Cloud) or build their own cloud. Normally, only large companies will build their own cloud due to the costs and complexity.
- There is no registration requirement for the use of public cloud services.
- If the foreign invested companies aim to provide cloud services as a commercial service to a third party or general public (like Amazon Cloud), they will face strict investment restrictions.
- Generally speaking, there should be no restriction for accessing the cloud from Germany and other parts of the world. However, the speed could be limited due to the Chinese Great Firewall. Furthermore, if the data stored on the cloud is to be transferred to a foreign server, regulations regarding cross-border data transfer should be followed. Further details can be found in Part 3.3.
- A list with major Chinese public cloud providers can be found in Part 3.4.

- There is a recommended standard regarding the selection of the cloud service providers for companies with different security levels. If clients or suppliers of the company are operators of key information infrastructure, the company should assess the expectations of the clients or suppliers with regard to data protection and security measures.

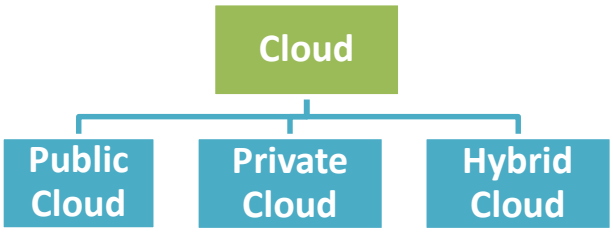
3. Detailed analysis

3.1. Can a company build its own cloud or should it use the services from a Chinese cloud provider?

3.1.1. Different kinds of clouds

Clouds can be divided into public clouds, private clouds and hybrid clouds.

- A public cloud shares resources and offers services to the public over the internet. The cloud resources (like servers and storage) are owned and operated by the cloud service provider and delivered over the internet. Public cloud services are provided by service providers, such as the state-owned telecommunication operators (China Mobile, China Telecom, China Unicom) or non-state-owned service providers such as Alibaba Cloud and Tencent Cloud.
- A private cloud offers computing services either over the internet or a private internal network only to select users instead of the general public. A private cloud can be physically located at the company, or it can be hosted by a service provider. But in a private cloud, the services and infrastructure are always maintained on a private network. Private cloud usually means that the company build its own cloud.
- The combination of a public cloud and a private cloud is a hybrid cloud.



(Different kinds of clouds)

3.1.2. Practical tips

Most of the companies choose to use services from a public cloud. However, in order to have a higher level of security and privacy standards, some companies choose to build their own private cloud. Due to the complexity and high costs, normally only large companies will set up their own private cloud.

From a legal perspective, it is allowed for companies to build their own private cloud. For example, it is encouraged by Chinese regulations (e.g. *Circular of the Ministry of Industry and Information Technology on the issuance of Guidelines for Promoting the Implementation of Enterprises on the Cloud)* that large companies may establish a private cloud with high data security requirements or consider setting up a hybrid cloud.

3.2. Should the use of cloud be registered in China?

3.2.1. Registration requirements for use of public cloud

Generally speaking, there is no registration requirement for using public cloud services (like Alibaba Cloud) in China.

However, if the company builds other functions based on the cloud services such as building its own website, then it should conduct the record filling obligation for the website ("ICP Filing") according to Art. 8 of the *Administrative Measures on Internet-based Information Services.*

(Example of a ICP Filing for a website)

3.2.2. Registration for building private cloud

There is no registration requirement for companies to build their own private cloud. However, the purpose of the private cloud shall be restricted to “own use” only.[1]

3.3. Are there any restrictions for the provision of cloud services in China?

Public cloud services belong to the Internet Data Center ("IDC") Services according to the *Promulgating the Classification Catalogue of Telecommunications Services*.

According to the current legal situation in China, foreign invested companies are not allowed to provide IDC services in China. Foreign companies (like Amazon) can only provide IDC services in China through local Chinese partners in the form of a technology cooperation. According to the CEPA agreement between Mainland China and Hong Kong, this sector is only accessible for foreign investors from Hong Kong and Macau, who still need a Joint Venture partner to offer public cloud services.

Public cloud providers (like Alibaba Cloud) shall meet the special requirements regarding registered capital, staff, premises and facilities and should obtain the corresponding business license for value-added telecommunications services (“ICP License”) according to Art. 3 Abs. 1 of the *Notice of Ministry of Industry and Information Technology on Cleaning up and Standardizing the Internet Network Access Service Market.*

The provision of services combined with the mere use of public clouds like Alibaba Cloud is not considered as a provision of cloud services to third parties. Example: In case a consultancy company for the automotive industry is providing services to its clients and is thereby using a public cloud like Alibaba Cloud (e.g. to store data for the clients), an ICP license would not be required.

[1] This has been confirmed by Mr. Zhang Jianhua (Director of Market Division, Information and Communication Administration Bureau, Ministry of Industry and Information Technology) during a public conference on July 25th, 2017.

Also, the ICP license is not to be confused with the ICP Filing for a website in China.

Using public cloud services	Building private cloud	Providing public cloud services
• No registration requried. • In case of building a website based on the public cloud, "ICP Filing" is requried.	• No registration requried. • Restrict to "own use" only.	• "ICP License" requried. • Currently not allowed for foreign investors

3.4. Can the cloud be visited from abroad?

3.4.1. Access

Generally speaking, there are no legal restrictions to access the data stored on clouds in China from abroad. However, due to the Chinese Great Firewall, access from abroad might be slow or unstable.

If the data stored on the cloud is to be transferred abroad, regulations for cross-border data transfer shall be followed (see below).

3.4.2. Cross border data transfer

Currently, there are no restrictions for the cross-border transfer of important data [2] and personal information [3] in place, except for operators of key information infrastructure according to Art. 37 of the Chinese *Cybersecurity Law* (see 3.5.2.).

However, there are several draft regulations dealing the with the cross-border data transfer of other entities that do not belong to the key information infrastructure. The cross-border transfer of personal information is subject to the *Draft Personal Information Protection Law* for example and the cross-border

[2] "Important Data" refers to data that is closely related to national security, economic development and societal interest and that, once disclosed without authorization, lost, abused, tampered with or destroyed, or aggregated, compiled and analyzed may lead to consequences e.g. regarding national security and defense, state property, administrative organs activities, critical infrastructure, state secrets, society, science or technology.

[3] "Personal Information" refers to various types of information that can be used separately or in combination with other information to identify a natural person, including but not limited to the name, date of birth, identity certificate number, personal biological identification information, address, telephone numbers, etc. of the natural person.

transfer of important data is stipulated in the *Draft Administrative Measures on Data Security*.

According to such draft regulations, a security assessment would need to be performed under specific circumstances before the data can be transferred abroad.

3.5. What are the major cloud providers in China?

The following list shows the top 10 Chinese public cloud providers in cloud computing market:

No. 1 Alibaba Cloud*

No. 2 Tencent Cloud**

No. 3 Huawei Cloud

No. 4 Baidu Cloud

No. 5 Jinshan Cloud

No. 6 JD Cloud & AI

No. 7 Inspur Cloud

No. 8 UCloud

No. 9 Yisu Cloud

No. 10 QingCloud

*Alibaba Cloud (https://www.aliyun.com), founded in 2009, is the biggest provider in cloud computing market in China.

**Tencent Cloud (https://cloud.tencent.com/), founded in 2013, holds the second place of the market share and has its strengths in the field of social media and games.

International cloud providers in the Chinese market are, for example, Amazon AWS, Microsoft Azure.

3.6. What else should companies pay attention to regarding the use of clouds?

3.6.1. Recommended standard for choosing a cloud provider

The recommended standard *Information security technology — Baseline for classified protection of cybersecurity* provides some security standards regarding the selection of cloud service providers. For example, according to Art. 6.2.5.1, for a company with the lowest security level, it is recommended that following requirements should be followed:

- *A cloud service provider with security compliance should be selected, and the cloud computing platform provided by it shall provide the corresponding registered security protection capability for the business application system carried by it;*
- *Various service contents and specific technical indicators of cloud services should be stipulated in the Service Level Agreement of the cloud service provider;*
- *The rights and responsibilities of cloud service providers should be stipulated in the Service Level Agreement, including the scope of management, division of responsibilities, access authorization, privacy protection, code of conduct, liability for breach of contract, etc.*

3.6.2. Operators of key information infrastructure

Operators of key Information Infrastructure have to comply with a higher level of security standards due to the nature of their business. According to Article 31 of the *Cybersecurity Law*, key Information Infrastructure includes “public communication and information service, energy, communications, water conservation, finance, public services and e-government affairs, and the key information infrastructures that may endanger national security, people’s livelihood and public interest in case of damage, function loss or data leakage on the basis of graded protection system for network security”.

If clients or suppliers of a company are operators of key Information infrastructure, the company should assess the expectations of the clients or suppliers with regard to data protection and security measures regarding using the cloud services.

4. List of important Laws and Regulations

4.1. Circular of the Ministry of Industry and Information Technology on the issuance of Guidelines for Promoting the Implementation of Enterprises on the Cloud (2018-2020), dated July 23, 2018

Article 5: "Large enterprises can establish private clouds and deploy key information systems with high data security requirements. The information system connecting customers, providers and employees can be deployed by public cloud, and the hybrid cloud architecture can be formed together with private cloud. For information systems with high data security requirements and need to provide services for external connection, a hybrid cloud architecture with data stored in private cloud and application deployed in public cloud can be considered."

4.2. Administrative Measures on Internet-based Information Services, dated January 8th, 2011

Article 8: "Whoever intends to engage in non-commercial internet-based information services shall apply for filing-for-record to the administrative organ in charge of telecommunications in the relevant province, autonomous region or directly administered municipality, or to the State Council department in charge of the information industry…"

4.3. Classification Catalogue of Telecommunications Services (Version 2015), dated March 1st, 2016

B11: "IDC services also include Internet resource collaboration services. Internet resource collaboration services refer to the data storage, Internet application development environment, Internet application deployment, operation and management services provided for users through the Internet or other network-related means featuring availability at any time, use as needed, expansion at any time and collaborative sharing, and by virtue of the equipment and resources established on the data center."

4.4. Notice of Ministry of Industry and Information Technology on Cleaning up and Standardizing the Internet Network Access Service Market, dated January 17th, 2017

Article 3: "Efforts should be made to carry out the requirements in capital,

personnel, place, facility, technical plan and information safety management specified in the Announcement of Ministry of Industry and Information Technology on Further Standardizing the Market Access of IDC and ISP Services (Gong Xin Bu Dian Guan Han [2012] No. 552, hereinafter referred to as "Announcement") to strengthen whole-process management including ex ante, interim and ex post management…"

4.5. Cybersecurity Law of the People's Republic of China, dated June 1st, 2017

Article 31: "For critical information infrastructure in important industries and sectors such as public communications, information service, energy, transport, water conservancy, finance, public service and e-government, and other critical information infrastructure that, once damaged, disabled or data disclosed, may severely threaten the national security, national economy, people's livelihood and public interests, the State shall give them extra protection on the basis of the graded system for cybersecurity protection. The specific scope and security measures for critical information infrastructure hall be developed by the State Council.

The State encourages network operators not engaged in critical information infrastructure to voluntarily participate in the protection system for critical information infrastructure."

Article 37: "The operator of a critical information infrastructure shall store within the territory of the People's Republic of China personal information and important data collected and generated during its operation within the territory of the People's Republic of China. Where such information and data have to be provided abroad for business purpose, security assessment shall be conducted pursuant to the measures developed by the CAC together with competent departments of the State Council, unless otherwise provided for in laws and administrative regulations, in which such laws and administrative regulations shall prevail."

4.6. Draft Personal Information Protection Law (2nd Draft for Comment), dated April 29th, 2021

4.7. Draft Administrative Measures on Data Security, dated May 28th, 2019

4.8. Information security technology — Baseline for classified protection of cybersecurity (GB/T 22239-2019), dated December 1st, 20

****

Your Contact in China:

Claudia Barkowsky
VDMA China Beijing Office
Chief Representative
Tel.: +86 10 8773 0210
Email: claudia.barkowsky@chinavdma.org

Your Contact in Germany:

Steffen Zimmermann
Leader Competence Center Industrial Security
Tel: +49 69 6603-1978
Email: steffen.zimmermann@vdma.org