CHINA: DATA PROTECTION & LOCALISATION, CYBER SECURITY LAW, VPN AND ENCRYPTION

BEITEN BURKHARDT

Introduction

Legal provisions concerning data protection and localisation requirements concerning personal as well as non-personal data can be found in various PRC laws and regulations, such as e.g. legislation addressing protection of personal information, transfer of data to overseas entities, legislation regarding cyber security, etc.

Legislation in China in this particular area is developing rapidly and besides existing legislation several new laws and regulations governing this topic are expected to be passed in the foreseeable future. For some potential future legislation already several subsequent drafts have been published and hence regular and thorough ongoing evaluation of IT compliance rules are paramount to ensure China businesses operate legally and securely.

1. Personal Data Protection

Matters relating to data localisation/transmission requirements of personal data are addressed in the PRC General Rules of Civil Law, the PRC Cyber Security Law, the Information Security Guidance on Protection of Personal Information of Public and Commercial Service Information Systems and other related laws and regulations:

PRC GENERAL RULES OF CIVIL LAW

The principle of personal data protection is stipulated in the "PRC General Rules of Civil Law" (《中华人民共和国民法总则》, "**Civil Law**"), which came into force on 1 October 2017. According to its Art. 111 "personal information of natural persons shall be protected by law. Any organisation or individual needing to obtain the personal information of other persons shall legally obtain and ensure the security of such information, and shall not illegally collect, use, process, or transmit the personal information of other persons, nor illegally buy, sell, provide, or publish the personal information of other persons."

- seek prior written consent (at least also in Chinese language for Chinese nationals) of each natural person subject to collection, usage, processing or transmission of such natural person's data, e.g. by using a consent form concerning the purpose, access, storage and transfer of such data

- disclose in such consent form for which purposes data are collected, who has access to such data and whether it will be transmitted to abroad

- ensure that personal data are kept secure, accessible only on a need-to-know basis and otherwise handled legally and within the scope of the given consent

- document that the business operator collecting the data has a legitimate business need to transfer personal data to abroad and that it has a robust and technically advanced IT system in place that keeps data secure, backed-up (potentially also in China so as to be able to prove localisation of data storage if this becomes necessary)

- apply state-of-the art technical measures to protect personal data from being leaked and accessed with ill intent

- regularly monitor and document that explorations are carried out to ensure that all Chinese legal requirements concerning data protection are followed and if necessary adjustment to the existing IT/data protection infrastructure is made

PRC CYBER SECURITY LAW

This is an important development of personal data protection in China. While the Civil Law remains silent on what acts/omissions constitute "illegal" obtaining of personal information, in order to be compliant with the above general rules, data users/business operators are well advised to ensure to take the following measures when collecting, storing and transferring personal data (whether domestically or from China to abroad):

The "PRC Cyber Security Law" (《中华人民共和国网络安全法》, "**Cyber Security Law**") came into effect on 1 June 2017 and addresses, amongst others, matters relating to offshore transmission of personal data.

Art. 37 Cyber Security Law stipulates that "personal information and important business data collected and generated in the operation of key information infrastructure operators within the PRC territory shall be stored within the [PRC] territory. Where it is necessary to provide such information and data to abroad due to business needs, security assessments shall be carried out according to the measures formulated by the National Internet Information Department in conjunction with the relevant departments of the State Council; if there are other provisions in laws and regulations, those provisions shall prevail."

Thus, a data localisation requirement under the Cyber Security Law applies only if all following criteria are fulfilled:

The data collected qualify as personal information or important business data collected in China

Art. 76 Cyber Security Law defines "personal information" as "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."

- Such data are necessary to be transmitted from China to abroad due to business needs

The Cyber Security Law (and to date no other PRC legislation publicly available and effective) does not define when such necessity due to business needs is established and there is no business-needs test definition otherwise defined under publicly available and effective Chinese law.

- Such data are collected and generated by "key information infrastructure operators"

Thus, a business would have to qualify as a "key information infrastructure operator" to fall under the realm of the data localisation requirement of Art. 37 Cyber Security Law. To that end, Art. 31 Cyber Security Law provides that "the State shall carry out special protection of important industries and fields, such as public communication and information services, energy, communication, water conservation, finance, public services and e-government affairs, and 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." Looking at such provision, the qualification of "key information infrastructures" is determined in particular from two perspectives, namely (i) certain industry sectors listed above, and (even beyond such industry sectors) (ii) information infrastructures that may have an impact on national/personal/public security interests.

The question what affects national, personal and public security interests in China tends to be one to which the answer is not necessarily firm, conclusive and permanent. This view is also reflected in the current Cyber Security Law which contains a clause that provides that "the detailed scope of and security protection measures for the key information infrastructures shall be formulated by the State Council."

Thus far, the State Council has not issued a binding guiding document on that matter. However, on 10 July 2017, the National Internet Information Department (i.e. the authority also mentioned in Art. 37 Cyber Security Law and being an organisation authorised by the State Council to take charge of the internet information content management), promulgated the "Regulations on Security Protection of Key Information Infrastructures (Draft)" (《关键信息基础设施安全保护条例(征求意见稿)》, "**Key Information Infrastructures Draft**"). While this is a draft only and hence not yet a promulgated effective piece of legislation, it may – in the absence of any other promulgated effective legislation – serve at this stage as a guidance as to what may be in the future be defined as a "key information infrastructure."

Art. 18 Key Information Infrastructures Draft outlines the criteria for "key information infrastructures" as "network and information systems operated by the following organisations:

- government authorities and units in the field of energy, finance, transportation, water conservancy, health care, education, social security, environmental protection, public utilities, etc.

- telecommunications networks, radio and television networks, internet and other information networks and units which provide cloud computing, big data and other large-scale information network services

- scientific research and production units in the field of national defense, science and technology, large-scale equipment, chemical industry, food and medicine, etc.

- news units such as radio stations, television stations and news agency, etc.

- other key entities."

Thus, business operators are required to assess the scope/purpose of their IT-Systems and the industry sector in which they are engaged in. Where the scope/purpose of their IT-Systems and the industry sector in which a business is engaged in falls under Art. 18 Key Information Infrastructures Draft, such business would qualify as "key information infrastructures", if such legislation would become effective as it stands now.

On 11 April 2017, the National Internet Information Department promulgated the Measures on the Security Assessment of Cross-border Transfer of Information and Important Data (Draft) (《个人信息和重要数据出境安全评估办法(征求意见稿)》, "**Security Assessment Draft**"). The Security Assessment Draft is a "Measure" in the sense of Art. 37 Cyber Security Law where it is provided that "security assessments shall be carried out according to the measures formulated by the National Internet Information Department in conjunction with the relevant departments of the State Council", hence laying out the conditions for the security assessment. This is thus far a consultation draft only and not yet a promulgated effective piece of legislation but would drastically expand data localisation and security assessment requirements. The Security Assessment Draft stipulates in its Art. 2 that "personal information and important business data collected and generated by network operators (网络运营者) within the PRC territory shall be stored within the PRC territory. Where it is necessary to provide such information and data to abroad due to business needs, a security assessment shall be carried out."

According to Art. 76 (3) Cyber Security Law, "network operators" (网络运营者) refers to "owners and managers of networks and network service providers" and Art. 76 (1) Cyber Security Law provides that "networks" refer to "systems composed of computers or other information terminals and relevant equipment that collect, store, transmit, exchange, and process information according to certain rules and procedures."

POSSIBLE IMPLICATIONS: DATA LOCALISATION AND SECURITY ASSESSMENT

If the infrastructure/hardware/system based on which a business operates in the PRC would be considered a "network" in the sense of the Security Assessment Draft (based on the rather vague definition of "network" in that draft pending further legal guidance) a data localisation requirement would become applicable to such business and the personal data transferred by it. With the currentwording of the Security Assessment Draft it would then be irrelevant if such business would qualify as "key information infrastructure operator" or not.

In addition, for any cross-border transfer of data (besides a business need), security assessments would then be needed to be carried out. The Security Assessment Draft provides in that regard that "network operators shall organise a security assessment for the data cross-border transfer before the data is transferred to overseas and shall be responsible for the result of such an assessment."

This wording suggests that one aspect of the security assessment entails company internal processes to set-up, maintain, keep secure and regularly check the data collection and transfer. In terms of the scope and key factors of such a security assessment, Art. 8 Security Assessment Draft provides as follows for personal data:

- necessity of the cross-border transfer
- information concerning personal data, including quantity, scope, type and sensibility of personal information and if the owner of the personal data has given consent to the transfer
- key information concerned, including quantity, scope, type and sensibility of the key information
- protection measures and ability level of the data receiving party and the network security standard of the country/region of the receiver
- risks of disclosure, damage, forgery or misuse after the cross-border transfer and re-transfer thereof
- risks to the national security, public interest and lawful personal interests caused by the cross-border transfer and aggregation of outbound information
- other important issues to be assessed

The Security Assessment Draft further provides that in the following cases network operators shall apply to the competent supervision authorities for cross-border data-transfers which would then be an additional layer of externally governed security assessment:

- personal information of more than 500,000 people is involved

- the transferred data volume exceeds 1,000 GB (it is unclear as of now if this is calculated accumulatively over a certain period or otherwise)

- the transferred data concerns nuclear facilities, chemical biological data, national personal information and important data by key information infrastructures operators

- network security data relating to key information infrastructures, including system vulnerabilities and security protection

- personal information and important data by key information infrastructures operators

- other circumstances that may affect national security or public interests

If the Security Assessment Draft would come into force as it stands now and depending in particular on how item (ii) is to be interpreted eventually, businesses that are considered network operators (or whoever would be considered as the network operator of the infrastructure/hardware/system based on which a business runs its IT transferring personal data), would have to seek the necessary government applications (in addition to fulfilling the data localisation requirement and the internal security assessment process).

PROHIBITION OF DATA TRANSFER

Art. 11 Security Assessment Draft prohibits the transfer of data collected or generated by network operators under the following circumstances:

- the outbound transmission of personal information has not obtained the consent of the information owner, or such transmission may infringe upon the owner's interests

- the outbound transmission of data would create a security risk in terms of national politics, economics, science and national defense, etc. and may affect the national security or harm the public interest

- authorities such as China Cyber Administration, public security authorities or national security authorities decide that the data shall not be transmitted to abroad

Art. 4 Security Assessment Draft also points out that "for cross-border transfer of personal information, personal information owners shall be notified of the purpose, scope, content, the recipient, as well as the country or region in which the recipient is located and shall consent to the transfer. The cross-border transfer of personal information of a minor must be consented by the guardian."

Looking at such Art. 4 and Art. 11 (i) and if the Security Assessment Draft would be enacted as it stands, businesses would be even more well advised to heed the requirement for consent and security measures as outlined above. Businesses therefore should regularly monitor

the development of the Security Assessment Draft being enacted/further developed and also if other relevant legislation comes into force in the future so as to ensure ongoing legal compliance.

INFORMATION SECURITY GUIDANCE ON PROTECTION OF PERSONAL INFORMATION OF PUBLIC AND COMMERCIAL SERVICE INFORMATION SYSTEMS (《信息安全技术公共及商用服务信息系统个人信息保护指南》, "GUIDANCE")

Besides the Cyber Security Law, the Guidance (promulgated by the National Committee of Information Security Standardisation Technology on 5 November 2012 and still in effect) governs the transfer of "personal information" from China to abroad. However, Art. 1 Guidance suggests that it should apply to service agencies for public and commercial purpose, e.g. in the fields of telecommunications, financial and medical services, etc. We hold that the Guidance, due to heavy restrictions in the specific industries they apply to and in particular after the Cyber Security Law has come into effect, should not be considered applicable to any company that has no direct public and/or commercial purposes.

2. Non-Personal Data Protection

Data localisation and transmission restrictions under PRC laws and regulations for non-personal data thus far only apply under the Cyber Security Law. As outlined above such restriction applies if all following criteria are fulfilled:

- The data collected qualify as personal information or important business data and are collected in China

The Cyber Security Law does not define what constitutes "important business data". Art. 17 Security Assessment Draft provides a definition for "important data" as "data closely related to national security, economic development and societal and public interests." It further reads that "the specific scope of the important data shall be determined with reference to relevant national standards and guidelines on important data identification." This definition is not helpful in terms of understanding what "important business data" would entail. We however take the view that "important data" seems more or less all refer to national-level interest data. Thus, we hold from a general perspective "important business data" should e.g. be data of a certain commercial value for which one would take measures to protect them and to keep them confidential. This could e.g. entail technical information and business information which is not known to the public, which is capable of bringing economic benefits to its legal owner, which has practical applicability, and which the legal owner has taken measures to keep secret (see also Art. 10 PRC Anti Unfair Competition Law which uses this definition for a "trade secret").

- Such important business data must be transmitted from China to abroad due to “business needs”

There is no business-needs-test defined under publicly available and effective Chinese law. Still, it could be reasonable to argue – until otherwise in the future a binding business-needs-test would be provided – that information collected in a business with international layout (e.g. having its headquarter outside the PRC) must from a perspective of operability, equality and fairness be able to transfer data from the headquarter to a subsidiary located in the PRC and vice versa.

- Such data are collected and generated by “key information infrastructure operators”

With the current wording of the Security Assessment Draft it would be irrelevant if a business would qualify as “key information infrastructure operator” or a “network operator” to fall under the scope of Art. 37 Cyber Security Law. Thus, if the infrastructure/hardware/system based on which a business operates in the PRC would be considered a “network” in the sense of the Security Assessment Draft (based on the rather vague definition of “network” in that draft pending further legal guidance) data localisation requirements would apply to such business and the important business data transferred by it. Further, businesses would have to seek government applications for outbound transfers (in addition to fulfilling the data localisation requirement and the internal security assessment process).

3. Safeguarding Data Transfers: VPN Access & Encryption

The current PRC legal framework regarding the internet and internet services such as VPN and encryption software is developing dynamically amid the PRC government‘s efforts to achieve its goal of “internet sovereignty”. Internet sovereignty refers to a concept whereas individual countries have the right to individually regulate the internet within their borders. Hence, PRC laws and regulations have to be assessed in such light. The use of VPN lines, encryption technologies and foreign internet gateways/MPLS lines are considered to be of high importance to many companies‘ business operations in the PRC in order to keep their business know-how and trade secrets safe or simply to connect to their headquarters located outside the PRC in a secure and reliant manner.

VPN ACCESS

VPN refers to an extension of a private network that encompasses links across shared or public networks like the internet. VPNs enable companies to transmit data between two endpoints across a shared or public network in a manner that imitates the properties of a point-to-point private link. Information concerning the set up and usage of VPN services can be found in various PRC laws and supplementing documents and can be outlined as follows:

- MIIT Notice on Cleaning Up and Regulating the Internet Access Service Market (《工业和信息化部关于清理规范互联网网络接入服务市场的通知》, "**Notice**")

The Notice was promulgated 17 January 2017 by the Ministry of Industry and Information Technology ("MIIT") and effective as of such date. Recently, this Notice received broad attention from foreign companies operating in China and was referred to as a piece of legislation rendering the use of VPN prohibited as of 31 March 2018.

The Notice addresses MIIT's local branches and telecommunication operators[1] and aims at "a nationwide work of cleaning up and regulating the internet access service market" during the period between 7 January 2017 and 31 March 2018 under the guidance of MIIT. While the Notice contains stipulations regarding VPN, it is however neither to be considered a formal law or regulation nor does it actually introduce novel stipulations but rather refers to already existing prior legislation. E.g. Chapter I. Notice ("Objective Tasks") re-emphasises the implementation of existing rules and regulations during the aforementioned period: "Relevant work shall be carried out to investigate and punish in accordance with the law the violations of laws existing at the markets of the internet data center (IDC) business, the internet service provider (ISP) business and content distribution network (CDN) business, such as conducting business without license, conducting business beyond scope of business and "multi-level sublease", effectively implement the subject responsibilities of enterprises, strengthen the administration over business license and access resources, intensify the administration over network information security, safeguard fair and sound market order and promote the healthy development of the industry."

Issues relating to VPN are e.g. addressed in Chapter II ("Focuses of Work"), Clause (II) ("Tightening resource administration and eradicating the use of resources in violation of regulations") No. 4. Here, it is provided that: "All basic telecommunications enterprises and internet access service enterprises shall conduct comprehensive self-inspection of their use of the network infrastructures and network access resources such as IP address and bandwidth and practically rectify the [following problems] problem of conducting cross-border business in violation of regulations: Without approval by the competent telecommunications authorities, no enterprise may construct or lease special circuits (including VPN (virtual private network)) and other telecommunications channels to conduct cross-border business activities. A basic telecommunications enterprise shall set up on centralised basis the profile of users to whom it leases international private lines and make it clear to the users that the lines are

[1] Communications administrations of all provinces, autonomous regions and municipalities directly under the Central Government, the China Academy of Information and Communications Technology, the China Telecommunications Corporation, the China Mobile Communications Corporation, the China United Network Communications Limited, the China Broadcasting and Television Network Co., Ltd, the CITIC Networks Co., Ltd., all business operators of the Internet data centers, business operators of the Internet access services and business operators content distribution networks.

for their use in office work internally and shall not be connected to domestic or overseas data center or business platform for telecommunications business activities."

The Notice therefore targets the following groups in terms of VPN use:

- **VPN Service Providers**, i.e. enterprises that aim at setting up and/or leasing VPN in the PRC to conduct cross-border business activities; these enterprises must obtain MIIT approval in order to lawfully offer VPN services; and

- **VPN Users**, i.e. enterprises using VPN; these shall only use VPN for internal business operation purposes but shall not use the VPN to connect to overseas (i.e. ex-China) data centers/business platforms for telecommunications business activities.

While the Notice itself does not make reference to specific existing legislation in regard to VPN, an explanatory statement to the Notice (**《工业和信息化部信息通信管理局负责人就《关于清理规范互联网网络接入服务市场的通知》答记者问》**) provided by MIIT during a press conference on 24 January 2017 ("**Conference**")[2], referred to the "Administration Measures for International Communication Gateway Exchanges" (**《国际通信出入口局管理办法》**, "**Exchange Measures**") promulgated by MIIT 26 June 2002 and effective 1 October 2002 in regard to the approval for setting up VPN to conduct cross-border business.

The Exchange Measures were formulated in regard to the setup of "international communications gateway exchanges" ("**ICGE**") and the engagement in international telecom services within the PRC (Art. 2 Exchange Measures). According to Art. 3 Exchange Measures, "ICGE" are defined as "international communications channel gateways, international communications service gateways, and international communications gateways in border areas." From the Exchange Measures, the following conclusions can be drawn in regard to VPN Providers and VPN Users:

VPN PROVIDERS:

In order to set up ICGEs, service providers shall apply with MIIT (Art. 4 Exchange Measures). Applications "shall be filed by *wholly State-owned telecommunications service operators*, and such telecommunications service operators shall also be responsible for the operation and maintenance thereof. (...). No organisation or individual may set-up, in any form, international communications gateways without the approval of the Ministry of Information Industry." Hence, ICGE can only be legally set-up by MIIT-approved PRC State Owned Telecommunication Service Providers. Such approved service providers may then lease private

[2] The following statement was made publicly available on MIIT's website: 《通知》关于跨境开展经营活动的规定，主要的依据是《国际通信出入口局管理办法》(原信息产业部令第22号)，规范的对象是未经电信主管部门批准，无国际通信业务经营资质的企业或个人，租用国际专线或VPN，私自开展跨境的电信业务经营活动。外贸企业、跨国企业因办公自用等原因，需要通过专线等方式跨境联网时，可以向依法设置国际通信出入口局的电信业务经营者租用, accessible under http://www.miit.gov.cn/n1146295/n1652858/n1653018/c5476695/content.html.

lines of international communications transmission channels to end-users (e.g. Companies) for point-to-point communication within a specified service scope and for internal use of such Companies only (excluding e.g. the right to operate telecom services (Art. 19 Exchange Measures)).

Qualified ICGE providers who lease private lines of international communications transmission channels are obliged to establish usersarchives. When setting up a VPN line through an ICGE, Art. 22 Exchange Measures provides that "The set-up of VPN via international internet gateways for the purpose of operating telecom services shall be reported to the MIIT for approval.

The setup of VPN for internal use via international internet gateways shall be filed with the MIIT for record." Based on information available with MIIT, currently China Telecom, China Mobile and China Unicom are approved by MIIT to provide ICGE/VPN services. Where an ICGE for international communication is set up without MIIT's approval or where a legally set up ICGE is used for VPN services outside the legally permissible scope, the respective service provider may be fined and/or the business operation may be closed (Arts. 26, 28 Exchange Measures). Thus, currently foreign enterprises operating in the PRC can legally only use a VPN provided by the MIIT approved providers China Telecom, China Mobile and China Unicom.

VPN USERS:

In regard to the use of VPN, two scenarios apply to foreign companies conducting business in the PRC and the on-/offshore transfer of data. The use of domestically (i.e. PRC) set up VPN Services or the use of non-domestically set up VPN Services.

USE OF DOMESTIC VPN:

Current PRC legislation addresses VPN set-up and lease within the PRC (domestic VPN) but does not target VPN set-up and lease outside the PRC (offshore VPN). Domestic VPN can be used subject to the following conditions being met:

- VPN are provided by MIIT-approved operators in accordance with Art. 4 Exchange Measures
- MIIT-approved operators have filed the set-up and lease of the VPN with MIIT and created respective VPN user profiles in accordance with Art. 22 Exchange Measures
- VPN are used for internal business needs only, Art. 22 Exchange Measures According to a statement of MIIT at the Conference, foreign trade enterprises, multinational enterprises and such may rent VPN lines from MIIT-approved ICGE providers and for internal business use requirements and the Notice and other existing laws and regulations shall not influ-

[3] 《通知》的相关规定不会对其正常运转造成影响, accessible under http://www.miit.gov.cn/n1146295/n1652858/n1653018/c5476695/content.html.

ence the normal business operation of such enterprises.3 If users disregard the usage limitation and carry out and operate telecom services, they may be fined and warned and in serious cases the responsible personnel may face criminal prosecution if the violation constitutes a criminal offense (Art. 30 Exchange Measures).

USE OF OFF-SHORE VPN:

Within the current PRC legal regime, the use of VPNs set-up and leased by companies outside the PRC is not explicitly addressed. Thus, one may hold that the use of such VPN lines is not generally in violation of PRC laws. However, such interpretation may face limitations considering the goals set forth in the Notice because MIIT may still step up its efforts to block use of VPNs that are not set up and leased by China Telecom, China Mobile and China Unicom.

ENCRYPTION TECHNOLOGY

The use of commercial encryption products in China is subject to the "Regulations on Administration of Commercial Cipher Codes" (《商用密码管理条例》, "**Administrative Regulations**"), effective as of 7 October 1999 issued by the State Council and the "Administrative Provisions on the Use of Commercial Encryption Products" (《商用密码产品使用管理规定》, "**Administrative Provisions**"), effective as of 1 May 2007, issued by the State Encryption Administration. Art. 5 Administrative Provisions allows the use of commercial encryption products for encryption protection and security certification of information that does not involve State secrets. Also, the use of commercial encryption products shall comply with State laws and shall not prejudice national interests, public interests, legitimate rights and interests of other citizens and shall not facilitate illegal and criminal activities.

Thus, the use of commercial encryption products is generally permissible under PRC laws subject to the above caveats. Where businesses do not violate the above caveats, there is no general legal restriction in China for using encrypted means of communication. The rule is however that in China only locally bought and approved encryption products shall be used. To that end Art. 6 Administrative Provisions requires that commercial encryption products used in the PRC shall be sold/purchased in China and must be approved by the Office of Security Commercial Code Administration ("**OSCCA**").

Encryption products that are developed and produced overseas and are not OSCCA approved shall in general not be used in China. OSCCA regularly publishes a catalogue of commercial encryption products approved to be sold in the PRC on a regular basis. There is however an exception to this rule offered in Art. 9 Administrative Provisions which provides that if foreign-invested enterprises ("**FIE**") due to genuine business needs must use encryption product produced outside China to communicate with and contact overseas parties, the FIE may use encryption products produced overseas subject to approval by OSCCA.

Further, pursuant to Art. 12 Administrative Provisions, "where the encryption product that a FIE applies to use needs to be imported from overseas, the foreign-invested enterprise shall apply for the Permit for Import of Encryption Products. Upon the entry of the encryption product, the foreign-invested enterprise shall make truthful declaration to the relevant customs office, and submit the Permit for Import of Encryption Products which shall be relied upon by the customs office in handling inspection and clearance procedures."

However, on 22 September 2017, the PRC State Council issued the "Decision on Cancelling a Group of Administrative Approval Matters" (《国务院关于取消一批行政许可事项的决定》, "**Decision**"), effective as of 29 September 2017, abolishing the aforesaid OSCCA approval procedure. Hence, based on the Decision, one could indeed argue that the aforesaid OSCCA approval procedure no longer applies. That said, according to the "Notice on Handing Over of Tasks after Cancelling Commercial Encryption Products Related Approval Matters" (《国家密码管理局关于做好商用密码产品生产单位审批等4项行政许可取消后相关管理政策衔接工作的通知》, "**Notice**"), issued by OSCCA as of 11 October 2017, "where the encryption product that a FIE applies to use needs to be imported from overseas, the FIE shall still apply for the Permit for Import of Encryption Products in accordance with Article 12 Administration Provisions." Such "Permit for Import of Encryption Products" can be obtained by submitting corresponding application documents to the competent Office of Security Commercial Code Administration at province level where the FIE locates. Based on additional information available with OSCCA, FIEs shall however still ensure that the domestic encryption product they intend to use in China is listed in the "Catalogue of Commercial Encryption Products Approved to Be Sold" regularly published by OSCCA. Thus, FIE are well advised to assess the following different situations:

- FIEs use encryption technology produced overseas and not available in China and which needs to be imported: There no longer exists an approval requirement with OSCCA, however the FIE shall apply for a "Permit for Import of Encryption Products" with the competent Office of Security Commercial Code Administration at province level

- FIEs use encryption technology produced overseas which is already available in China: There no longer exists an approval requirement with OSCCA, however the FIE shall confirm with the importer that a "Permit for Import of Encryption Products" for such encryption products has been duly obtained

- FIEs uses domestic (i.e. PRC) encryption products: The FIE shall ensure that the product is listed in the "Catalogue of Commercial Encryption Products Approved to Be Sold" regularly published by OSCCA

Susanne Rademacher
German Attorney-at-law | Partner
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH
Beijing

Dr. iur. Jenna Wang-Metzner
Legal Consultant | Partner
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH
Beijing

Simon Henke
German Attorney-at-law | LL.M.
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH
Beijing

Corinna Li
Legal Consultant | LL.B. | LL.M.
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH
Beijing

Kata Liu
Legal Consultant | LL.B. | LL.M.
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH
Beijing

BEIJING | BERLIN | BRUSSELS | DUSSELDORF | FRANKFURT AM MAIN
HAMBURG | MOSCOW | MUNICH | ST. PETERSBURG

WWW.BEITENBURKHARDT.COM

03/2020