LLINKS Law Offices
通力律师事务所

上海
上海市银城中路 68 号
时代金融中心 16 楼和 19 楼
邮编：200120
电话：+86 21 3135 8666
传真：+86 21 3135 8600

SHANGHAI
16F/19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
邮编：100005
电话：+86 10 8519 2266
传真：+86 10 8519 2929

BEIJING
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话：+852 2592 1978
传真：+852 2868 0883

HONG KONG
27F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

伦敦
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

LONDON
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com
master@llinkslaw.com

Llinks Corporate and M&A Bulletin
June 2019

Seeing through the Mist
—— A Review of Personal Information Export Security Assessment Measures (Draft)

By David Pan | Stella Huang

On June 13, the State Cyberspace Affairs Commission ("**CAC**") issued the *Personal Information Export Security Assessment Measures (Draft)* (the "**Draft Measures**") to seek public comments. Prior to the Draft Measures, CAC in April 2017 issued the *Personal Information and Important Data Export Security Assessment Measures (Draft)* (the "**2017 Draft Measures**"), which for the first time specifically aimed to regulate the export of personal information and important data. Comparing the Draft Measures with the 2017 Draft Measures, both the law enforcement authority and underlying regulatory logic have significantly changed, and the Draft Measures provide for much more detailed regulation on personal information export security assessment. In this article, Llinks Cybersecurity and Data Service Team will, based on its own rich experience and insights in this area, interpret the Draft Measures from 1) law enforcement authority; 2) the obligees and object of the assessment; 3) the contracts between personal information providers and recipients; 4) assessment

如果您需要本出版物的中文本，
请与下列人员联系：

郭建良: +86 21 3135 8756
Publication@llinkslaw. com

For more Llinks publications,
please contact:

Roy Guo: +86 21 3135 8756
Publication@llinkslaw. com

Llinks Law Offices
www. llinkslaw. com

requirements and 5) legal liabilities, as well as a clause by clause comparison between the provisions of the Draft Measures and the provisions on personal information of the 2017 Draft Measures.

1. Law Enforcement Authority

The 2017 Draft Measures provide that data export will be supervised and coordinated by the CAC and implemented by the authorities in charge of relevant industries. The aforementioned authorities are generally understood as government authorities that execute their regulatory powers on relevant industries such as transportation and education. The Draft Measures change the implementing authority to provincial CAC offices. The responsibilities of provincial CACs in personal information export security assessment include: arranging for experts to conduct security assessment; inspecting on the cybersecurity status of network operators' personal information export; receiving personal information export reports from network operators, etc. The state CAC is in charge of settling network operators' complaints, and reviewing the assessment results reached by provincial CACs.

2. Obligees and Object

a) Obligees

According to the Draft Measures, those who directly or indirectly bear the obligations of personal information export security assessment include network operators, personal information recipients and foreign organizations.

i. Network Operators

The *Cyber Security Law* (the "CSL") limits the obligees to conduct security assessment for the export of personal information and important data to critical information infrastructure operators ("CIIO"). The 2017 Draft Measures expand the scope of obligees to include all network operators. Subsequently, some internal unofficial discussion drafts after the 2017 Draft Measures intended to limit the scope to CIIOs. However, the Draft Measures followed the approach of the 2017 Draft Measures by requiring all network operators to bear personal information export assessment obligations.

The *Legislation Law* provides that no departmental regulations shall, without the authorization by laws or regulations, decisions or orders issued by the State Council, reduce the rights or expand the obligations of citizens, legal persons or other organizations, or increase the powers or decrease the legal responsibilities of the department. Although the CSL does not require network operators other than CIIOs to conduct security assessment, the 2017 Draft Measures quoted another upper law, the *National Security Law*, to legitimately expand such obligations to all

network operators. In contrast, the Draft Measures expand the obligations to all network operators by referring to the CSL only, which makes its legislative basis questionable.

ii. Personal Information Recipients

In the context of personal information export, personal information recipients should be an important party to conduct security assessment. However, due to the fact that such data recipients are located outside the PRC, it is practically difficult to directly regulate the recipients. Therefore, the Draft Measures mandate the clauses of the contract entered into between data providers and data recipients, so as to impose obligations and responsibilities on the recipients in an indirect way.

iii. Foreign Organizations

The Draft Measures provide that where foreign organizations collect personal information of PRC users and export such personal information, they shall fulfill their network operator obligations through their legal representatives or entities within the PRC.

b) Object

The Draft Measures define personal information within their meaning "electronic information or information otherwise recorded that can independently or in combination with other information identify a natural person". The definition is identical to the definitions in the CSL and the 2017 Draft Measures, but is inconsistent with the broader definitions in applicable judicial interpretations and the personal information national standards, which include information related to personal activities.

3. Contracts between Personal Information Providers and Recipients

Among others, GDPR regulates personal information related activities through standard contract clauses (SCC). Similar to the GDPR methodology, the Draft Measures stipulate that network operators should submit their contracts with recipients when filing for personal information export security assessments. The clauses of the contract are one of the key aspects of safety assessments. The network operator must also report the performance of the contract to provincial CACs.

The Draft Measures stipulate the contract clauses from the following four aspects and determine the necessary clauses of the contract: the basic clauses of the contract, the obligations of personal information providers, the obligations of personal information recipients, and the re-transfer by personal information recipients.

a) Basic Clauses of the Contract

The Draft Measures stipulate that the contract shall specify: the purpose, type, and overseas retention time for information export; the personal information subject being the beneficiary of contract clauses concerning the rights and interests of the personal information subject; that the network operator or recipient shall compensate for the damage suffered by the personal information subject, unless it is proved that it has no liability; and that the contract shall be terminated or security assessment shall be re-conducted when it is difficult for the information recipient to perform the contract.

b) Obligations of Personal Information Providers

The contract shall stipulate the following obligations of the personal information provider: to inform the personal information subject about the export of personal information; to provide a copy of the contract at the request of the personal information subject; and to make the advance compensation when the personal information subject is unable to obtain compensation from the recipient.

c) Obligations of Personal Information Recipients

The contract shall stipulate the following obligations of the personal information recipient: to provide access to, correction and deletion of personal information for the personal information subject; to use and retain personal information in accordance with the contract; and to notify the provider in time when the performance of the contract is affected by changes of law.

d) Re-transfer by Personal Information Recipients

For the re-transfer activities by the recipient, the Draft Measures stipulate that the network operator shall inform the personal information subject of the re-transfer; if personal sensitive information is involved, the consent of the personal information subject shall be obtained; if personal sensitive information is not involved, the consent of the personal information subject is not required, but the personal information subject may request to stop the transfer; and if the legitimate rights and interests of the personal information subject are damaged due to re-transfer, the network operator shall assume the liability of advance compensation.

The above necessary clauses mostly focus on the legitimate rights and interests of personal information subject from the perspective of the subject's right to know and right of consent. The necessary clauses also protect the rights and interests of personal information subject through the joint and several liability of the network operator, that is, if the legitimate rights and interests of the personal information subject are damaged, the network operator will assume joint and several liability with the recipient or the third party which receives personal information to the personal information subject. The Draft Measures stipulate that

the contract should also clarify that "when the legitimate rights and interests of the personal information subject are damaged, he can claim compensation from the network operator or the recipient or both parties by himself or by the agent, and the network operator or the recipient should compensate, unless it is proved that it has no liability." Understandably, this provision aims to better protect the subject by reversing the burden of proof in the case of damage to the rights and interests of the personal information subject. Debatably, however, there may be legal obstacles to the realization of this purpose because the existing law has not yet explicitly taken cases of infringement of personal information as an exception to the general principle of "who advocates, who has the burden of proof".

The effect of supervising information recipients through contract may be limited. Because of the privity of contract, if the information provider exports personal information without security assessment, the contract that does not meet the requirements of the Draft Measures is still valid between the provider and the recipient; even if the clauses of the contract meet the requirements of the Draft Measures, if the contracted recipient has a lighter liability for breach of contract, or the provider or the personal information subject cannot effectively obtain compensation due to obstacles of judicial procedure, the recipient would actually breach the contract at a lower cost.

4. Specific Requirements for Security Assessment

a) Triggering of Obligations

The 2017 Draft Measures stipulate that network operators should organize assessment on their own before data export. In cases of data export that may affect national security and social public interests (for example, containing or accumulating personal information of more than 500,000 people or containing population health information), the network operators should report to the competent authorities in charge of relevant industries for security assessment.

In contrast, the Draft Measures stipulate the obligation of network operators to file for mandatory security assessment without quantitative or qualitative preconditions. In order to lighten the burden of filing of network operators, the Draft Measures stipulate that it is not necessary to repeat assessment for multiple or continuous provision of personal information to the same recipient. Undoubtedly, this regulation is a relief for multinational companies which have regular needs of data export. However, although the recipients are the same, every two years or when the purpose, type and overseas retention time of personal information export changes, the risk of data export will change greatly, the assessment should be re-filed and re-conducted.

b) Analysis Report

When a network operator files for security assessment of personal information with CACs, it should provide not only the filing form and the contract with the recipient, but also the analysis report of the

security risk and security safeguard measures of personal information export. The network operator should be responsible for the authenticity and accuracy of the reports.

The main contents of the analysis report include: (1) the background, scale, business, finance, reputation and network security capabilities of the network operator and the recipient; (2) personal information export plan, including the duration, the number of subjects involved, the scale of personal information exported, whether personal information will be transferred to third parties after export, etc.; and (3) personal information export risk analysis, and measures to protect personal information security and the legitimate rights and interests of the personal information subject.

c) Implementation of Assessment

i. From Self-assessment to Filing for Assessment

As commented above, comparing with the 2017 Draft Measures, the Draft Measures change the data export requirements on network operators from "self-assessment" to "filing for assessment", which imposes network operators a stricter compliance obligation.

ii. Contents of Assessment

In the process of assessment, the CAC will organize experts or technician forces to conduct security assessment which focuses on the filing form, the contract signed with the data recipient, the analysis report of the security risk and security safeguard measures of personal information export submitted by the network operator.

The security assessment includes the following key aspects: (1) whether the data export is in compliance with relevant laws, regulations and policies; (2) whether the contract clauses are designed to fully safeguard legitimate rights and interests of personal information subjects; (3) whether the contract can be effectively performed; (4) whether the network operator or data recipient has a history of damaging legitimate rights of personal information subjects, or has experienced severe cybersecurity accidents; (5) whether the network operator acquires the personal information lawfully and appropriately; (6) other factors which need to be assessed. It can be seen that the recipient's security capabilities and the protection of the personal information subject's legal rights are the top priority in the security assessment.

iii. Time Limit of Assessmen

The 2017 Draft Measures provide that the security assessment organized by authorities in charge of relevant industries shall be completed in sixty working days. The Draft Measures reduced the time limit to fifteen working days, which will undoubtedly increase efficiency and prevent business arrangements of network operators from being interrupted.

d) Prohibited Export

The Draft Measures stipulate that the CAC may require the network operator to terminate or suspend the data export out of the following situations: (1) where there is relatively severe data leakage and data misuse incidents of the network operator or data recipient; (2) where it is impossible or difficult to maintain the legitimate rights and interests of personal information subjects; (3) where network operators or data recipient is unable to protect the security of personal information. Whether a network operator or data recipient has ever experienced a relatively severe data security incident is one of the measurement dimensions of its data security capabilities. If there has been a data security incident, the data export will more likely be banned. For the measurement of personal information security capability, please refer to the *Information Security Technology - Data Export Security Assessment Guideline (Exposure Draft)*.

e) Record, Report and Inspection

To impose follow-up supervision on data export, the Draft Measures also set forth requirements on maintaining personal information export records for at least 5 years. Such records should include the time of export, identity of the information recipient, and type, amount, degree of sensitivity of the information.

In addition, network operators shall report to the CACs annually the conditions of personal information export and contract performance. The CACs shall regularly make inspection on the aforementioned conditions.

5. Legal Liabilities

The Draft Measures stipulate that, if a network operator violates the provisions of these Measures to export personal information, it shall be punished in accordance with relevant laws and regulations. This is a quite general provision. In order to understand the relevant legal responsibilities stipulated by the complex cybersecurity legal regime, readers can refer to relevant practical articles in the 30 Questions About the CSL compiled and written by Llinks Cybersecurity and Data Service Team, such as Summary of Companies' Responsibilities and Obligations under the CSL, On Criminal Liabilities of Network Operators.

6. Conclusions

The Draft Measures provide detailed provisions on the personal information export security assessment, and sets mandatory security assessment obligations on companies, which consist of unprecedentedly strict requirements. For network operators with personal information export needs, compliance measures should be taken as early as possible to ensure the legitimate rights and interests of personal information subjects; to review the security capabilities of personal information recipients in advance; and to track the full cycle of the exported data.

Appendix

Clause by Clause Comparison between the *Personal Information and Important Data Export Security Assessment Measures (Draft)* and the *Personal Information Export Security Assessment Measures (Draft)*

No.	Topic	The *Personal Information and Important Data Export Security Assessment Measures (Draft)*	The *Personal Information Export Security Assessment Measures (Draft)*	Main Changes
Existing Rules				
1.	Legislative Purpose	**Article 1** These Measures are formulated in accordance with the **National Security Law of the People's Republic of China**, the Cyber Security Law of the People's Republic of China, and other laws and regulations to protect the security of personal information and important data, safeguard cyberspace sovereignty, national security, and social and public interests, as well as legitimate rights of citizens, legal persons and other organizations.	**Article 1** These Measures are formulated in accordance with the relevant laws and regulations such as the Cyber Security Law of the People's Republic of China for the purpose of protecting the security of personal information in data export.	Revision of current rules; Deleting "These Measures are formulated in accordance with the National Security Law"
2.	Principle	**Article 2** The personal information and important data generated or collected by a network operator during its operations within the territory of the People's Republic of China **shall be stored within China**. If it is	**Article 2** When network operators export personal information collected during operations within the People's Republic of China (hereinafter referred to as the "personal information export"), they shall conduct security	Revision of current rules; Deleting the requirement that "Personal information collected during domestic

		necessary to export data due to business needs, security assessment shall be conducted according to these Measures. **Article 3** Security assessment for the data to be exported shall be conducted under the principles of **fairness, objectivity and validity**.	assessment in accordance with these Measures.	operations shall be stored within China"
3.	Consent of Personal Information Subjects	**Article 4** For personal information export, an explanation on the purpose, scope, content and recipient of the data to be exported, and the country or region where the recipient is located shall be given to personal information subjects, and the export shall be consented by such subjects.	N/A	Deletion of current rules
4.	Authorities in Charge	**Article 5** The state cyberspace administration shall conduct overall coordination for security assessment for the data to be exported, and guide authorities in charge of relevant industries to conduct security assessment for the data to be exported. **Article 6** An authority in charge of relevant industries shall take charge of the security assessment for the data to be	**Article 10** **The provincial cyberspace administrations** shall **regularly organize the inspections** of the conditions of personal information export such as operators' records of personal information export, with the focus on inspecting the performance of the obligations stipulated in the contracts.	Revision of current rules

		exported in respect of the industry, and shall **organize regular security inspections** for the data to be exported in respect of the industry.		
5.	Requirements on Security Assessment	**Article 7** Prior to data export, a network operator shall **organize on its own security assessment** for the data to be exported, and be liable for the assessment results. **Article 9** Listing of circumstances where a network operator shall **file with authorities in charge of relevant industries to organize security assessment**. **Article 12** A network operator shall, in light of its business development and network operations, conduct security assessment for the data to be exported **at least once a year**, and shall r**eport the assessment information to authorities in charge of relevant industries** concerned without delay.	**Article 3** Before personal information export, network operators shall **file with the local provincial cyberspace administrations for security assessment for personal information export**. To provide personal information to different recipients, security assessment shall be filed for separately, and multiple or continuous provision of personal information to the same recipient do not need to go through multiple assessment. New security assessment shall be carried out every two years or in case of changes of the purpose of personal information export or the type or overseas storage period of such information.	Revision of current rules; Changing from "security assessment organized by network operators in principle" to "security assessment filed with CACs in principle"
6.	Key Contents to Be Assessed	**Article 8** Listing of aspects that shall be highlighted during the security assessment for the data to be exported.	**Article 6** Listing of aspects that shall be highlighted during the security assessment for the personal information to be	Revision of current rules

			exported.	
7.	Time Limit of Security Assessment	**Article 10** The security assessment organized by an authority in charge of relevant industries shall be completed **within 60 working days**.	**Article 5** Security assessment shall be completed **within 15 working days**, and the time limit may be appropriately extended for those with complex situations.	Revision of current rules; The time limit for CACs' security assessment is reduced from 60 working days to 15 working days
8.	Reporting Security Assessment Results	**Article 10** The security assessment results shall be made known to the network operator, and **reported to relevant departments of the state cyberspace administration**.	**Article 7** When the provincial cyberspace administrations inform network operators of the results of security assessment for personal information export, they shall simultaneously **report the results of security assessment for personal information export to the state cyberspace administration**.	Reiteration of current rules
9.	Prohibited/Suspended Personal Information Export	**Article 11** Data shall not be exported in any of the following circumstances: (1) The export **fails to obtain the consent of personal information subjects**, or may jeopardize personal interests; (2) The export may affect national security and jeopardize social and public interests; or (3) Other data which are forbidden to be exported as determined by relevant	**Article 2** If it is identified by the security assessment that the personal information export **may affect national security or damage public interests, or that it is difficult to effectively protect the security of personal information**, such information export shall not be allowed. **Article 11** In case of occurrence of any of the following situations, the	Revision of current rules

		authorities.	cyberspace administrations may require network operators to **suspend** or terminate personal information export: (1) Network operators or recipients have encountered serious data breach and data misuse incidents; (2) **Personal information subjects cannot or find it difficult to safeguard the legitimate rights and interests of individuals**; or (3) **Network operators or recipients cannot protect the security of personal information**.	
10.	Reporting	**Article 13** In the event of data export in violation of relevant laws and regulations, or these Measures, any individual or organization may report to the state cyberspace administration, public security authority or other relevant authorities.	**Article 12** Any individual or organization shall have the right to report to the cyberspace administrations at the provincial level or above or to relevant departments the acts of personal information export violating the provisions of these Measures.	Reiteration of current rules
11.	Legal Liabilities	**Article 14** Violations to these Measures shall be penalized in accordance with relevant laws and regulations.	**Article 18** Network operators that export personal information in violation of the provisions of these Measures shall be punished in accordance with relevant laws and regulations.	Reiteration of current rules
12.	International Treaties	**Article 15** If the Chinese government has entered into any agreement on the data to be exported with other nations	**Article 19** If there are clear provisions on personal information export in the treaties or agreements that China has acceded to or	Reiteration of current rules

		or regions, such agreement shall be followed. The information involving state secrets are subject to relevant regulations.	concluded with other countries, regions and international organizations, these provisions shall apply. However, the articles about which China has stated its reservations are exceptions.	
13.	Applicability to Other Entities	**Article 16** These Measures are applicable mutatis mutandis to the security assessment for the export of the personal information and important data generated or collected by other individuals and organizations within the territory of the People's Republic of China.	N/A	Deletion of current rules
14.	Definitions	**Article 17** "Personal information" refers to all the information recorded in electronic form or otherwise, which can be used, solely or together with other information, to determine the identity of a natural person, including but not limited to the name, date of birth, ID card number, personal biometric information, address and phone number of the natural person.	**Article 21** "Personal information" refers to all the information recorded in electronic form or otherwise, which can be used, solely or together with other information, to determine the identity of a natural person, including but not limited to the name, date of birth, ID card number, personal biometric information, address and phone number of the natural person.	Reiteration of current rules
New Rules				
15.	Filing Materials for Security Assessment	N/A	**Article 4** Network operators shall provide the following materials for security assessment for personal	New rules

			information export, and shall be responsible for the authenticity and accuracy of the materials: (1) Application form; (2) **Contracts entered into between network operators and recipients**; (3) **Analysis reports of the security risk and security safeguard measures of personal information export**; and (4) Other materials required by the state cyberspace administration.	
16.	Compliant	N/A	**Article 7** If network operators have any objections to the results of security assessment for personal information export of the provincial cyberspace administrations, they may **file complaints** with the state cyberspace administration.	New rules
17.	Retention of Personal Information Export Records	N/A	**Article 8** Network operators shall establish records of personal information export and keep the records **for at least five years**. The records shall include the following contents: (1) The date and time when personal information is exported; (2) The identity of the recipients, including but not limited to the recipients' names, addresses, contact	New rules

			information, etc.; (3) Types, quantities and sensitivity level of personal information exported; and (4) Other contents as stipulated by the state cyberspace administration.	
18.	Reporting Personal Information Export Conditions	N/A	**Article 9** Network operators shall, before December 31 of each year, report **the conditions of personal information export and contract performance in the current year** to the local provincial cyberspace administrations. Occurrence of **serious data security incidents** shall be reported to the local provincial cyberspace administrations in a timely manner.	New rules
19.	Contract Clauses	N/A	**Article 13** Contracts or other legally binding documents signed by network operators and personal information recipients (collectively referred to as "contracts") shall specify the following contents: (1) Purposes of personal information export and the types and storage periods of such information; (2) Information subjects are the beneficiaries of the terms in the contracts that involve the rights and interests of personal information subjects;	New rules

			(3) When the legitimate rights and interests of personal information subjects are damaged, **network operators or recipients shall make compensation, unless it is proved that they have no liability**; (4) **If changes of the legal environment in the recipients' countries make it difficult to perform contracts, contracts shall be terminated, or security assessment shall be re-conducted**; **Article 14** It shall be specified in the contracts that **network operators** assume the following **responsibilities and obligations**: (1) **Informing personal information subjects** of the basic information of network operators and recipients as well as the purposes of personal information export and the types and storage periods of such information; (2) **Providing the duplicate of contracts** at the request of personal information subjects; and (3) Forwarding the appeals of personal information subjects to receipients upon requests, including making claims to recipients; **if personal**	

			information subjects cannot get compensation from recipients, network operators shall pay the compensation in advance. **Article 15** It shall be specified in the contracts that **recipients** assume the following **responsibilities and obligations**: (1) Providing means for personal information subjects to access their personal information. When personal information subjects request correction or deletion of their personal information, recipients shall make response, correct or delete relevant information at a reasonable cost and within a reasonable time limit. (2) Using personal information in accordance with the purposes specified in the contracts, and the overseas storage periods of personal information shall not exceed the time limit specified in the contracts. (3) Confirming that the acts of signing the contracts and fulfilling the obligations in the contracts will not violate the legal requirements of the countries where the recipients are located. **When the changes in the legal**	

			environment of the recipients' countries and regions may affect the execution of the contracts, recipients shall notify network operators in a timely manner, and then network operators shall report the situations to the provincial cyberspace administrations where network operators are located. **Article 16** It shall be specified in the contracts that **recipients shall not transmit the personal information received to any third parties** unless the following conditions are met: (1) Network operators have, by means of e-mail, instant messaging, letter or fax, **informed personal information subjects** of the purposes of exporting the personal information to third parties, the identity and country of third parties, the types of personal information exported, and the periods for storage of the personal information by third parties; (2) Recipients declare that they shall, **when the information subjects request them to stop transmitting to the third party**, stop the transmission and request the third party to destroy the	

			personal information that has been received. (3) **If personal sensitive information is involved, the consents from personal information subjects have been obtained**; or (4) If the transmission of personal information to third parties causes damage to the legitimate rights and interests of personal information subjects, **network operators shall agree to assume the liability for compensation in advance**.	
20.	Analysis Reports of Security Risk and Security Safeguard Measures	N/A	**Article 17** Listing of the contents of the network operators' analysis reports of security risk and security safeguard measures for personal information export.	New rules
21.	Collection of Domestic Personal Information by Foreign Organizations	N/A	**Article 20** When foreign organizations, in the course of their business operations, **collect personal information of domestic users** through the Internet, they shall, through legal representatives or organizations, fulfill the responsibilities and obligations of network operators stipulated in these Measures within the territory of China.	New rules

Contact Details

If you would like to know more information about the subjects covered in this publication, please feel free to contact the following people or your usual Llinks contact.

Author	
David Pan Tel: +86 21 3135 8701 david.pan@llinkslaw.com	

Shanghai	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	**Bernie Liu** Tel: +86 21 3135 8678 bernie.liu@llinkslaw.com
Selena She Tel: +86 21 3135 8770 selena.she@llinkslaw.com	**Nicholas Lou** Tel: +86 21 3135 8783 nicholas.lou@llinkslaw.com
Dali Qian Tel: +86 21 3135 8676 dali.qian@llinkslaw.com	**Kenneth Kong** Tel: +86 21 3135 8777 kenneth.kong@llinkslaw.com
David Wu Tel: +86 21 6043 3711 david.wu@llinkslaw.com	**David Pan** Tel: +86 21 3135 8701 david.pan@llinkslaw.com
Elyn Jiang Tel: +86 21 6043 3710 elyn.jiang@llinkslaw.com	
Beijing	
David Yu Tel: +86 10 8519 2266 david.yu@llinkslaw.com	**Bernie Liu** Tel: +86 10 8519 2266 bernie.liu@llinkslaw.com
Yuhua Yang Tel: +86 10 8519 1606 yuhua.yang@llinkslaw.com	
Hong Kong(in Association with Dennis Fong & Co., Solicitors)	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	**Sandra Lu** Tel: +86 21 3135 8776 sandra.lu@llinkslaw.com
London	
Yuhua Yang Tel: +44 (0)20 3283 4337 yuhua.yang@llinkslaw.com	