LLINKS Law Offices 通力律师事务所

Shanghai
19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
Tel: (86 21) 3135 8666
Fax:(86 21) 3135 8600

Beijing
Unit 401, China Resources Building
No. 8 Jianguomenbei Avenue
Dongcheng District
Beijing 100005 P.R.China
Tel: (86 10) 8519 2266
Fax:(86 10) 8519 2929

上海
上海市银城中路68号
时代金融中心19楼
邮政编码: 200120
电话: (86 21) 3135 8666
传真: (86 21) 3135 8600

北京
北京市东城区建国门北大街8号
华润大厦401单元
邮政编码: 100005
电话: (86 10) 8519 2266
传真: (86 10) 8519 2929

www.llinkslaw.com
master@llinkslaw.com

Llinks Corporate and M&A Bulletin
April 2017

Brief Analysis on the Measures for the Security Assessment of the Export of Personal Information and Important Data (Exposure Draft)

By Wayne Chen, David Pan and Tianhang Li

On 11 April 2017, the State Internet Information Office of China issued the Notice on Seeking Public Comments on Measures for the Security Assessment of the Export of Personal Information and Important Data (Exposure Draft) (hereinafter referred to as the **"Measures"). Exposure Drafts for public comment usually differ only slightly from the final official versions according to the history and practice of legislation in China. Therefore, companies should timely anticipate the implementation and enforcement of the new law and arrange compliance work in advance with help of this analysis and discussion on the contents of the Measures. Based on the contents of the 18 articles contained in the Measures, we believe the following aspects deserve your attention.**

1. Legislative Basis of the Measures: the State Security Law and Cyber Security Law

i). Article 1 of the Measures clearly states that it is enacted based on the *State Security Law of the People's Republic of China* (hereinafter referred to as the **"*State Security Law*"**), the *Cyber Security Law of the People's Republic of China* (hereinafter referred to as the **"*Cyber Security Law*"**), and other laws and regulations, and these laws provide the legislative basis for the Measures to the extent of defining which information needs to undergo an assessment if the information needs to be transmitted abroad as personal information and important data. Article 16 of the *State Security Law* provides that the state "protects life and property safety and other legitimate interests of citizens", suggesting that personal information is in its nature both data and a civil interest. Article 25 of the *State Security Law* stipulates that the state shall maintain a "safe and controllable network and core information technology, critical infrastructure and information

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

If you would like other Llinks publications, please contact:

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

Llinks Law Offices
www.llinkslaw.com

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

systems and data in key areas", suggesting that important data should be such "information system and data of critical infrastructure and important sectors". **So the Measures are not merely a detailed and corresponding implementation of Article 37 of the *State Security Law*.** Such knowledge is beneficial for us to carry out the requirements for the export of data and to defend the cyber sovereignty and security of China.

2. Regulated Subject: the Meaning of Network Operator

According to Article 2[1] of the Measures, the regulated subject of the Measures is "network operator". The definition of "network operator" is in conformity with the definition in the *Cyber Security Law*, which is "owners and managers of network and network service providers." Mr. Heqing Yang, the Deputy Director of the Economic Law Office of the NPC Legislation Work Committee points out in "The Understanding of the Cyber Security Law of the People's Republic of China" (in his role as chief editor) that "the concept of network service provider, which includes Internet Service Provider (ISP) and Internet Content Provider (ICP), was used more often in the laws before the implementation of *Cyber Security Law*. Apart from the internet, the concept of network in the *Cyber Security Law* also includes local area network and industrial control system. They do not directly provide commercial or public services for the community, but the owner and controller shall undertake relevant safety obligations to prevent cyber safety risks and maintain the stability of cyber operations." **It is worth nothing that the concept of "network operator" may be broader than "network service provider".**

Authority	Regulation	The Concept Adopted
Legislative Authorities	*Cyber Security Law* (Order of the President No. 53)	Network Operator
Administrative Authorities	"Regulations on the Protection of Rights to Information Network Communication" (Order of the State Council No. 634)	Network Service Provider
	"Administrative Measures for Internet Information Services" (Order of the State Council No. 588)	Internet Information Service Provider
Judicial Authorities	"Provisions of the Supreme People's Court on Several Issues concerning the Application of Law to Trial of Civil Dispute Cases of Infringement of Personal Rights via Information Networks" (Fa Shi [2014] No. 11)	Network Service Provider

"Internet Information Service Provider"<"Network Service provider"<"Network Operator"

In addition, **Article 16 of the Measures provides that "these Measures are applicable *mutatis mutandis* to the security assessment for export of other personal information and important data generated or collected by other individuals and organizations within the territory of the People's Republic of China." Therefore, besides network operators, the Measures apply to all relevant individuals and entities.**

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

3. The Application of the Regulations: Scope, Conduct and Subjects.

(1) Scope of Application

According to the definition in the Measures, export of data refers to providing overseas institutions, organizations and individuals with the personal information and important data generated or collected by network operators during their operations within the territory of the People's Republic of China. Regarding the meaning of "within the territory", two points should be noted.

Firstly, the meaning of "territory" mainly depends on the definition of geographical space (territorial location). Chinese mainland is "within the territory" while "overseas" refers to other countries and the regions of Hong Kong, Macao and Taiwan.

Secondly, the meaning of "within the territory" in the sentence "the personal information and important data generated or collected by network operators during their operation within the territory of the People's Republic of China" is not clear. Does it mean that the network operator is located within the territory? Does it mean that the server "generating and collecting" information and data is located within the territory? Or does it mean that the customer from whom the network operator collects such information or data (data subject) is located within the territory? The Measures do not provide specific answers. As we understand it, the word "operation" has a broad meaning; simultaneously the internet itself has a cross-border attribute; and the combination of "within the territory" and "operation" could cause ambiguity. Upon the *Cyber Security Law* officially coming into force, such ambiguity may be clarified in judicial cases or in detailed rules promulgated by relevant authorities.

<table>
<tr><th>Expression in the Article</th><th>Query</th><th>Rationale for Discussion</th></tr>
<tr><td rowspan="4">"The personal information and important data generated or collected by network operators during their operation within the territory of the People's Republic of China"</td><td>Whether it is applicable to a network operator whose place of office is not within the territory?</td><td rowspan="4">The legal status of "information" is not clear in the present law, while it focuses on the protection the collection and use of personal information. It is still not clear whether the information is attached to the customers from whom the information is collected, or to storage media or to the collector in practical scenarios.</td></tr>
<tr><td>Whether it is applicable to a network operator whose place of office is within the territory while the server generating and</td></tr>
<tr><td>collecting information and data is not?</td></tr>
<tr><td>Whether it is applicable to a network operator if the customer from whom the network operator collects information and data (data subject) is not located within the territory?</td></tr>
</table>

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

In addition to the applicability problem from a territorial perspective, we should also pay attention to where the Measures rank in terms of priority. Regarding the applicable law for the export of data, according to Articles 2, 15[2] and 16[3] of the Measures combined with Article 37[4] of the *Cyber Security Law* and Article 25 of the State Security Law, we can come to the following conclusions.

Firstly, comparing Article 2 of the Measures, Article 37 of the *Cyber Security Law* and Article 25 of the *State Security Law*, we understand that the former is a normative document which elaborates on the latter two. Therefore, after the Measures become effective with some amendments probably, network operator should first look into the Measures for guidance on data export.

Secondly, after the Measures become effective later with some amendments probably, any treaties on the export of data signed by the PRC government and any other country or region, specific regulations regarding state secrets export or other specific provisions concerning the export issues of individuals and organizations prevail over Measures.

<table>
<tr><th>Sequence of application (First)</th><th>Sequence of application (Second)</th><th>Sequence of application (Last)</th></tr>
<tr><td>agreement on export of data signed by the PRC government and any other country or region</td><td rowspan="3">The Measures to be officially adopted with some amendments probably【stronger operability】</td><td rowspan="3">Article 37 of Cyber Security Law and Article 25 of State Security Law【more principled, weaker operability】</td></tr>
<tr><td>specific regulations regarding state secrets</td></tr>
<tr><td>other specific provisions concerning export issues of individuals and organizations</td></tr>
</table>

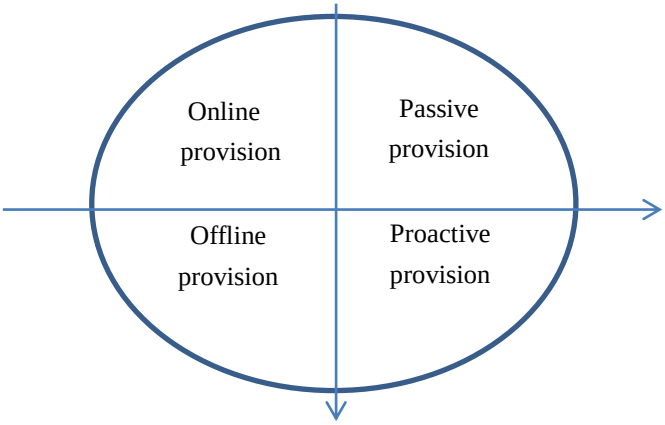
(2) Applicable Conduct

Based on the definition in the Measures, the Measures shall apply to network operators “providing” relevant information and data. In practice, "providing" includes proactively and passively providing, and providing online and offline. To better understand the meaning of the word "provide", we consider the following two points are worth noting.

Firstly, “providing” in this context means the network operators directly transmitting relevant information or data through the network to overseas institutions, organizations, or individuals. If the network operator allows the foreign body access to read the relevant information or data through the network, it is in effect the same as providing proactively. Therefore, "passive provision" will also be regulated under the Measures.

Secondly, although the language of "export of data" suggests it applies to a network, Article 1[5] of the Measures clarifies that the legislative basis for the Measures includes the *Cyber Security Law* and the *State Security Law*. Most likely, the Measures to be officially adopted will not apply to offline export of data. For example, it would be controversial for civil aviation staff to check the rationality and legitimacy of information or data storage media belonging to passengers in airport security checks. However, when reading the Measures literally, we cannot rule out the possibility that the Measures will also cover offline export of data.

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.



【Note】Arrow direction represents the applicability of the Measures to be officially adopted, from strong to weak.

(3) Applicable Object

Here, the "applicable object" is a broad concept which includes "personal information and important data" (subject matter), and "the institutions, organizations, individuals outside the territory" (object). With regard to our understanding of "personal information and important data", we believe that the following two points are worth noting.

Firstly, "personal information" here does not refer to information about a person, but refers to identifiable information relating to a person. Such a concept is relatively narrow. Specifically, the Measures follow the definition in the *Cyber Security Law* and state that “personal information” refers to all kinds of information by means of electronic records or other means to identify personal identity separately or combined with other information, including but not limited to a natural person’s name, date of birth, ID card number, personal identification information, address, telephone number, etc. Therefore, “desensitized” personal information to the effect of being non-identifiable does not belong to the personal information defined in the Measures. Nevertheless, if huge amounts of such “desensitized” information make it possible for information recipients to obtain data that is closely related to national security, economic development and the social public interest, such information may be regarded as "important data".

Secondly, the exact content of the "important data" here depends on subsequent promulgation of the "relevant national standards and important data identification guidelines". We understand that the provisions in the *Cyber Security Law* on “important data” establish the basic principles for the export of data. The Measures to be finally adopted after amendments will further clarify the disposal process (assessment and reporting, etc.), while the connotation of "important data" may be explained by government level policies first and then be regulated specifically in the laws and regulations. Before the promulgation of relevant regulations, we recommend that readers look into relevant commentary published on CAC website (official website of the Office of the Central Leading Group for Cyberspace Affairs, link: http://www.cac.gov.cn/) as well as international practice.

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

Cyber Security Law (Already introduced)	**Measures for the Security Assessment of the Export of Personal Information and Important Data (Seeking public comments)**	**Important data identification guidelines (to be introduced)**
Establishes the basic principles of disposal of export of data	Clarifies the disposal process (assessment, reporting, etc.)	Clarifies the connotation of "important data" (which is the boundary of government supervised information)

To understand the meaning of "the institutions, organizations, individuals outside the territory", we shall further elaborate on the word "institution". From a broad perspective, "institutions" include government agencies. In practice, if the network operator needs to provide relevant information or data to government agencies outside the territory, such conduct may involve the application of two or more laws. Bilateral or multilateral treaties regarding the export of data described above will resolve the problem to a certain extent, but before the introduction of specific treaties, the network operator will still need to follow China's laws and regulations regarding data export according to the territorial principle. If there is any provision for data transmission outside China and it conflicts with regulations in China, we recommend that the relevant network operators timely communicate with the network administration authorities to clarify the relevant regulations or the applicable conditions or circumstances for exemption from the assessment procedure.

4. The Pre-Conditions of the External Assessment: Prohibitive Provisions and Initialization Conditions

Article 11[6] of the Measures specifies the circumstances where data shall not be transmitted abroad, including if (1) the export of data is not approved by the person identified by the personal information or the custodian of a minor identified by the personal information, or may jeopardize personal interests; or (2) the export of data causes security risks to the nation's political system, economy, technology or defense, which may affect national security and jeopardize social and public interests. Article 111 of the *General Rules of the Civil Law of the People's Republic of China* (hereinafter referred to as the "***General Rules of the Civil Law***"), which was recently issued, stipulates that any organization or individual may lawfully obtain the personal information of others where necessary and ensure the safety of such personal information, and shall not illegally collect, use, process or transmit the personal information of others, or illegally buy or sell, provide or make public the personal information of others. In addition, according to the provisions of standard terms in the *Contract Law of the People's Republic of China*, we understand that in the process of collecting and producing information, network operators should follow the relevant provisions when drafting authorization terms in electronic form. Furthermore, "affecting national security and jeopardizing social and public interests" is a relatively broad concept. Network operators should clearly define such circumstances in the risk warning and undertaking clause when signing contracts concerning the export of data.

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

The Circumstances where Data shall not be Transmitted Abroad	Relevant Laws and Regulations	Contract Terms which Network Operators should Consider
The export of data is not approved by the person identified by the personal information or by the custodian of a minor identified by the personal information, or may jeopardize personal interests	*Cyber Security Law* *General Rules of the Civil Law*	Standard terms of licensing and authorizing
The export of data causes security risks to the nation's political system, economy, technology or defense, which may affect national security and jeopardize social and public interests	*Cyber Security Law* *State Security Law*	Risk warnings and undertaking clause

Article 9[7] of the Measures provides the initialization procedures for the security assessment. This article explicitly stipulates the conditions (in terms of the scale, content, importance etc. of the data) for the security assessment prior to the data being transmitted abroad.

Types	Conditions	Requirements
The scale of the data	Contains individually or in aggregate the personal information of more than 500,000 people	In any of these circumstances, a network operator shall apply to its industrial authority or regulator to organize a security assessment
The volume of the data	Exceeds 1,000 gigabytes (GB)	
The content of the data	Concerns nuclear facilities, chemical biology, national defense industry, population and health, etc.	
Environmental information contained in the data	Large-scale project activities, marine environment and sensitive geographic information	
The security, technology and substantial content of critical information infrastructure	System vulnerabilities, security protection and other cyber security information of critical information infrastructure	
	A critical information infrastructure operator provides personal information and important data abroad	

5. Two Levels of the Assessment: National and Individual

Article 8[8] of the Measures provides the key content of the security assessment for the data to be transmitted abroad. Article 8(1) points out the "necessity of transmitting the data abroad". At present, the Measures are in the process of seeking public comments. We do not know the legislators' opinions on "necessity". Therefore, it is unknown whether the data which does not need to be transmitted abroad can pass the security assessment. According to Article 3 of the Measures, security assessments for the data to be

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

transmitted abroad shall be conducted under the principles of impartiality, objectivity and efficiency to protect the security of personal information and important data, and to promote the orderly and free flow of network information. Therefore, we understand that the legislators' opinion on the data to be transmitted abroad should be neutral, and will focus on balancing the competing interests of data security and the free flow of information. At the same time, the Measures do not clarify the handling procedures after the assessment. From the original intention of the legislation, the handling procedures after the assessment do not merely follow two outcomes, one where the data can be transmitted abroad and the other where the data cannot be transmitted abroad. We suggest that the data should be allowed to be transmitted abroad with some relevant measures implemented by the network operators according to the assessment status. We hope the handling procedures will be clarified in subsequent legislation.

The Key Content of the Security Assessment for the Data to be Transmitted Abroad	
Necessity of transmitting the data abroad (Article 8(1))	
Condition of personal information (Article 8(2))	Condition of Important data (Article 8(3))
Qualifications of the data recipient and the cyber security environment of the country or region where the data recipient is located (Article 8(4))	
Risks to the data after being transmitted abroad and after being further transferred (Article 8(5))	Risks of gathering the data to be transmitted abroad (Article 8(6))

6. The Mechanism of the Assessment: the Subjects, Modes and Requirements

Articles 5 through 7 and 12 of the Measures specify the subjects, modes and requirements of the security assessment. The mechanism of security assessment mainly includes internal assessment, external assessment, annual assessment, and second assessment.

Mechanism of the Assessment	**Relevant Provisions**	**Specific Requirements**	
Internal assessment	Aritcle7[9]	Prior to transmitting data abroad, a network operator shall organize on its own the security assessment for the data to be transmitted abroad, and shall be liable for the assessment results.	
External assessment	Article 5[10] Article 6[11]	The cyberspace authorities	Overall coordination
		Industrial authority or regulator	In charge of the security assessment and organize regular security inspections
Annual assessment	Article 12[12]	In light of its business development and network operation, the network operator shall conduct a security assessment for the data to be transmitted abroad at least once a year	
Second assessment	Article 12	In case of any changes to the data recipient, any major changes to the purpose, scope, quantity and type of the data transmitted abroad, or any major security events occurring in relation to the data recipient or the data to be transmitted abroad, another security assessment shall be conducted by the network operator without delay.	

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

The network operators' internal assessment, annual assessment and second assessment are all self-assessments. Network operators apply these self-assessment methods except for conditions concerning Article 9 and Article 11 of the Measures. Therefore, network operators' abilities and qualifications of self-assessment will have an impact on their normal operations.

7. Several Suggestions

We conclude this discussion paper with the following suggestions in relation to data transmitted abroad.

Firstly, the issue of cyber security has received high attention from our government, and has been regulated on the level of "cyber sovereignty". Network operators or other enterprises involving network operation should conduct compliance review of their own cyber security as soon as possible, especially those companies which are planning to obtain financing or planning to invest capital in the network technology area. We suggest treating cyber security as one of the important issues of compliance and due diligence.

Secondly, the security assessment for the data to be transmitted abroad involves self-assessment. For those operators which are relatively weak in their qualifications and compliance, we suggest hiring external professional agencies to conduct individual assessments in order to reduce risks.

Thirdly, there is a provision about "agreement on the export of data with other nations or regions" in the Public Consultation for the Draft Measures on the Due Diligence of Non-resident Financial Account Information in Tax Matters (Exposure Draft) which the State Administration of Taxation drafted and announced at the end of 2016, and this provision is also mentioned in the Measures. We understand that the idea of data-centric asset management is growing at the national level, and we suggest that network operators and other enterprises involving network operations respond actively at the level of corporate management to the frequent changes in the external circumstances of politics and business.

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

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	
Wayne Chen Tel: (86 21) 3135 8766 way.chen@llinkslaw.com	**David Pan** Tel: (86 21) 3135 8701 david.pan@llinkslaw.com
Tianhang Li Tel: (86 21) 3135 8652 tianhang.li@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
Beijing	
David Yu Tel: (86 21) 3135 8686 david.yu@llinkslaw.com	**Bernie Liu** Tel: (86 21) 3135 8678 bernie.liu@llinkslaw.com
Yuhua Yang Tel: (86 10) 8519 1606 yuhua.yang@llinkslaw.com	
Hong Kong(in Association with Vivien Teu & Co)	
David Yu Tel: (86 21) 3135 8686 david.yu@llinkslaw.com	**Sandra Lu** Tel: (86 21) 3135 8776 sandra.Lu@llinkslaw.com

© Llinks Law Offices 2017

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

1 Article 2 of the Measures for the Security Assessment of the Export of Personal Information and Important Data (The Measures): the personal information and important data generated and collected by a network operator during its operation within the territory of the People's Republic of China shall be stored within Chinese territory. For the information and data that is indeed necessary to be transmitted abroad due to business needs, security assessment shall be conducted according to the Measures.

2 Article 15 of the Measures for the Security Assessment of the Export of Personal Information and Important Data (The Measures): if the Chinese government has entered into any agreement on the export of data with other nations or regions, such agreement shall prevail. The information involving state secrets shall be dealt with according to relevant regulations.

3 Article 16 of the Measures for the Security Assessment of the Export of Personal Information and Important Data (The Measures): the Measures are applicable *mutatis mutandis* to the security assessment for export of other personal information and important data generated or collected by other individuals and organizations within the territory of the People's Republic of China.

4 Article 37 of *Cyber Security Law of the People's Republic of China*: Key information infrastructure operators shall store personal information and important data gathered and produced during operations within the territory of the People's Republic of China. Where it is really necessary to provide such information and data to overseas parties due to business requirements, a security assessment shall be conducted in accordance with the measures formulated by the national cyberspace administration authority in concert with the relevant departments under the State Council. Where the laws and administrative regulations provide otherwise, those provisions shall prevail.

5 Article 1 of the Measures for the Security Assessment of the Export of Personal Information and Important Data (Exposure Draft): the Measures are hereby enacted in accordance with the *State 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 for the purpose of protecting the security of personal information and important data, safeguarding cyberspace sovereignty, national security, and social and public interests, as well as promoting the orderly and free flow of network information.

6 Article 11 of the Measures for the Security Assessment of the Export of Personal Information and Important Data (Exposure Draft): data shall not be transmitted abroad in any of the following circumstances: (1) The export of data is not approved by the person identified by the personal information, or may jeopardize personal interests; (2) The export of data causes security risks to the nation's political system, economy, technology or defense, which may affect national security and jeopardize social and public interests; or (3) Other data which are forbidden to be transmitted abroad as determined by the cyberspace administration, public security administration, security authority and other relevant authorities.

7 Article 9 of the Measures for the Security Assessment of the Export of Personal Information and Important Data (Exposure Draft): in any of the following circumstances, a network operator shall apply to its industrial authority or regulator to organize security assessment: (1) The data to be transmitted abroad contains individually or in aggregate the personal information of more than 500,000 people; (2) The volume of the data to be transmitted abroad exceeds 1,000 gigabytes; (3) The data to be transmitted abroad contains data in relation to nuclear facilities, chemical biology, national defense industry, population and health, as well as the data of large-scale project activities, marine environment and sensitive geographic information; (4) The data to be transmitted abroad contains system vulnerabilities, security protection and other cyber security information of critical information infrastructure; (5) A critical information infrastructure operator provides personal information and important data abroad; or (6) Other data which may affect national security, and social and public interests, and are necessary for assessment as determined by the industrial authority or regulator. If there is no responsible industrial authority or regulator, the cyberspace administration shall organize the assessment.

8 Article 8 of the Measures for the Security Assessment of the Export of Personal Information and Important Data (Exposure Draft): during security assessment for the data to be transmitted abroad, assessment in the following aspects shall be prioritized: (1) The necessity of transmitting the data abroad; (2) The condition of the personal information involved, including the quantity, scope, type and sensitivity of the personal information, as well as whether the person identified by the personal information agrees to transmit his/her personal information abroad; (3) The condition of the important data involved, including the quantity, scope, type and sensitivity of the important data; (4) The security protection measures, ability and proficiency of the data recipient, as well as the cyber security environment of the country or region where the data recipient is located; (5) Risks of leakage, damage, tampering and abuse of data after being transmitted abroad and after being further transferred; (6) Risks to national security, social and public interests, and personal legitimate interests arising from transmitting the data abroad and gathering the data to be transmitted abroad; and (7) Other important matters to be assessed.

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

9 Article 7 of the Measures for the Security Assessment of the Export of Personal Information and Important Data (Exposure Draft): prior to transmitting data abroad, a network operator shall organize on its own the security assessment for the data to be transmitted abroad, and shall be liable for the assessment results.

10 Article 5 of the Measures for the Security Assessment of the Export of Personal Information and Important Data (Exposure Draft): the cyberspace administration shall conduct overall coordination for security assessment for the data to be transmitted abroad, and guide industrial authorities or regulators to conduct security assessment for the data to be transmitted abroad.

11 Article 6 of the Measures for the Security Assessment of the Export of Personal Information and Important Data (Exposure Draft): an industrial authority or regulator shall be in charge of the security assessment for the data to be transmitted abroad in respect of the industry, and shall organize regular security inspections for the data to be transmitted abroad in respect of the industry.

12 Article 12 of the Measures for the Security Assessment of the Export of Personal Information and Important Data (Exposure Draft): a network operator shall, in light of its business development and network operation, conduct a security assessment for the data to be transmitted abroad at least once a year, and shall report the assessment information to the industrial authority or regulator concerned without delay. In case of any changes to the data recipient, any major changes to the purpose, scope, quantity and type of the data transmitted abroad, or any major security events occurring in relation to the data recipient or the data to be transmitted abroad, another security assessment shall be conducted without delay.

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.