LLINKS Law Offices
通力律师事务所

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

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

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

LONDON
1/F, 3 More London Riverside,
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 432

Llinks Law Bulletins | Corporate and M&A

January 2020

Top Five Points for MNCs for Compliance with APP DP Rule

By Xun Yang

The Cyberspace Administration of China, the Ministry of Industry and Information Technology, the Ministry of Public Security, and the State Administration for Market Regulation jointly issued the *Notice on Sanctions against Illegal Collection and Use of Personal Data on APPs* (the "***APP DP Notice***") on 25 Jan.2015. They further released the *Measure for Determining Illegal Collection and Use of Personal Data* (the "***APP DP Measure***") on 28 November 2019. The APP DP Notice and the APP DP Rule elaborate the non-compliant practice surrounding the collection and use of personal data on Apps and provide guidance for network operators to comply their data protection practice with the PRC laws.

By taking reference to these rules regarding collection and use of personal information on Apps and also to our services to multinational companies, we summarize the top five points for compliance with the APP data protection rules.

For more Llinks publications, please contact:

Publication@llinkslaw.com

I. A mere translation of GDPR based privacy policy does not comply with the PRC law in China

Many MNCs have their "global" privacy policies based on GDPR and wish to customize them for applications in the PRC. This is, of course, a reasonable practice. However, it would be important to note that, although GDPR represents the historically highest standard for data protections, a translation of a privacy policy based on GDPR may not satisfy the PRC law requirements for the reasons below:

- The terminologies and mechanism under GDPR are different from those under the PRC laws. For example, the PRC law does not have the concept of "data controller." The use of GDPR terminology or mechanism may make the privacy policy not clear enough to meet the PRC law requirements;
- Chinese language is quite different from English or other European language. A direct translation may not be user friendly and cause confusing, and thus violate the clarity requirement under the PRC data protection laws.
- There are certain PRC unique data protection requirements in relation to operations of Apps or other online services which are not available under GDPR, including, for instance, notification to government of data leakage and provision of communication channels.

II. Data protection is not only about privacy policy; rather, it concerns the design and operation of the Apps

We often receive instructions to review and amend privacy policies and user agreements, which are of course legal works. However, it would be important to bear in mind that data protection is not only about privacy policies; and design of the Apps and data protection practice are at least equally important. For MNCs which build quite sophisticated APPs, given Chinese mindsets are different from westerners', the design of Apps which works under GDPR may not be considered compliant in the PRC. The loopholes in relation to designs and operations include:

- lack of obvious links to the privacy policy on the page where personal data are collected;
- lack of clear indications to channels by which users can request for a copy, deletion, or update of their personal data; and
- lack of function to de-register users' accounts.

Please note, depending on the levels of sophistication of target users, the standards for determining "obviousness" and "clearness" vary. Generally speaking, however, access to privacy policy through four successive links would likely to considered not obvious or clear.

III. Data protection policies and practice must be customized for Chinese users and China market

MNCs usually operate their IT systems and process their data on a global basis, with IT and back office functions deployed offshore. This of course is an efficient operational model and maximizes data values. As far as collection and use of data on Apps are concerned, the policies and practices for data protection must reflect this arrangement and align this arrangement with the PRC law requirements. The typical loopholes include:

- the privacy policy was written in such a European centric manner that it elaborate the export of data outside of Europe but not address whether data collected in China would be exported outside of China;
- the contact number by which users can report data leakage or request for a copies, deletion or amendment of personal data are foreign numbers; and
- the privacy officers who take charge of responding to users' reports or requests do not speak Chinese.

The extent to which foreign developed APPs must be customized for Chinese users and for the China market would depend on the sophistication levels of the target users and the way the relevant Apps are marketed.

IV. Scope and purpose of collection and use of personal information must be sufficiently clear to render users meaning freedom to decide whether to grant consents

Informed consent is a data protection requirement under both GDPR and the PRC law, of which both require data collectors to clearly inform data subjects of the scope and purpose of data collections. However, the practical level of clarity requirements is different between GDPR and the PRC law.

A balance between clarity and flexibility needs to be maintained in describing the scope and purpose of collection. A too narrow and too specific description will result in any change in the App triggers an amendment to the existing privacy policy and the necessity to seek consents to such amendment. On the contrary, too vague descriptions may not be compliant. The following descriptions are often seen in MNCs' privacy policies for Apps which may not be sufficiently clear under the PRC law.

- Failure to elaborate the consequence if users decline to provide their personal data as requested;
- Lack of clear definition of scope of collection and, instead, using of summative descriptions such as "contact information," "information about your health conditions" etc;
- Failure to clearly inform users of the purpose of collection by only stating that the collection of certain personal information is necessary to enjoy the services provided on the Apps; and
- To include unexhausted descriptions, such as "all legitimate purpose" in the purpose of collection, which does not provide users with any clue regarding why users' personal data are to be collected.

- In particular, when an App is operated on a global basis, how and for what purpose personal data can be collected and used are different by jurisdictions. Reference to the scope defined in any legislation in a foreign jurisdiction may not be considered a sufficient disclosure.

V. Device ID, location information, and other information describing users' behaviors need to be considered

Under GDPR, personal data are defined as "any information relating to an identified or identifiable natural person" whilst Europe has specific legislation regulating cookies and other non-personal or machine information. PRC law does not have specific legislations on cookies but the scope of personal data is broadly defined to include the information which describes under behaviors. Therefore, certain rules in relation to machine information (e.g., device code, location information, viewing histories without identifying specific persons) which are usually included in cookie policies in Europe may need to be addressed in privacy policies in China.

If you would like to know more information about the subjects covered in this publication, please contact:

Xun Yang
+86 21 3135 8799
xun.yang@llinkslaw.com

For any further questions on this subject or other business consultation, please feel free to contact us: master@llinkslaw.com

SHANGHAI	BEIJING	HONG KONG	LONDON
T: +86 21 3135 8666 F: +86 21 3135 8600	T: +86 10 8519 2266 F: +86 10 8519 2929	T: +852 2592 1978 F: +852 2868 0883	T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD