Llinks Client Alert – Cybersecurity, Data & Privacy

November 2020

Shanghai · Beijing · Shenzhen · Hong Kong · London

LINKS Law Offices
通力律师事务所

I. Legislation

On October 21st, the Standing Committee of National People's Progress issued the heated debated *Draft Personal Information Protection Law* for public consultation. The Draft Personal Information Protection Law has 8 chapters, including the general principles, the rules for processing personal information, the rules for cross-border transmissions of personal information, the right of personal information subjects in processing, the obligations of personal information controllers, the department responsible for personal information protection, the legal liabilities and the annex.

Llinks Comment: The Draft Personal Information Protection Law, without any doubt, has been the legislation attracting most discussions recently. As the first comprehensive legislation in the personal data protection regime, it has clarified a few controversial legal issues:

Firstly, it creates an extraterritorial jurisdiction in the legal regime of personal information protections, i.e. foreign entities are also required to abide by the requirements under the Personal Information Protection Law when they collect personal information from individuals residing in China.

Secondly, it sets out reasonable rules for the "engaged processing" of personal information, which boost the legitimate movement of personal information.

Thirdly, the Draft Personal Information Protection Law reshaped the regulatory framework for the export of personal information, which sets out different requirements on the exportation of personal information based on whether the data exporter is an operator of critical information infrastructure, and whether the volume of data to be exported reaches a statutory threshold to be provided for. These requirements not only maintain the security of personal information when they are transferred overseas but also facilitate data cross-border transmissions for multi-national companies having operations in China.

Lastly, the Draft Personal Information Protection Law further clarifies the concept of "data sovereignty", which means any provision of personal data to foreign governments or foreign authorities due to judicial assistance or enforcement assistance, must be approved by Chinese government in advance..

On October 20th, the State Administration for Market Regulation released the *Administrative Measure for the Supervision on E-commerce (Draft)* (the "**E-commerce Measure**") for public consultation. As the implementing rule of *PRC E-commerce Law*, the E-commerce Measure further specifies the requirements on the registration of business operators, the responsibilities and obligations of e-commerce platforms and various statutory notification obligations.

On October 20th, MIIT issued the *Notice on Strengthening the In-process and Afterwards Regulation on Foreign-invested Telecom Enterprises*, which summarizes the specific requirements on the entrance permission and local operation requirements which foreign-invested telecom enterprises must comply with after the abolishment of "Foreign Investment Review" procedure, including to strictly conform to the *Administrative Measures for the Operation Permission of Telecom Services*, to perform the annual filing obligations for the telecom services operation information regularly, to report the corresponding monitoring information regarding the telecom services market according to the relevant laws etc.

II. Court Rulings

Ms Ting CHEN, a student studying in Shanghai, claimed that her privacy was infringed by Baidu because when she used Baidu Tieba App, Baidu pushes advertisements to her by illegitimately utilizing her personal information and misusing her location information. She determined to file a suit against the operator of Baidu Tieba App, i.e. Beijing Baidu Network Technology Co., Ltd. After more than 4 months' dispute on the venue of litigation, Hubei Huanggang Middle People's Court final decided that this case would be heard by Hubei Jinchun People's Court and the first hearing would be conducted publicly in the near future.

III. Law Enforcement

As of Oct. 14th, during the "CLEAN NET 2020" dedicated actions, Zhangjiakou Public Security Bureau has deleted 792 pieces of illegal information, taken down illegal 263 mobile applications and shut down 5 mobile applications, as well as imposed administrative penalties on 724 entities which failed to perform the network security protection obligations. Typical examples which Zhangjiakou Public Security Bureau released include a government agency responsible for public health management in Economic Development District, Zhangjiakou City failed to perform network security obligations in terms of the Multi-level Protection Scheme requirement, resulting in its official website contains cybersecurity vulnerabilities, as well as a trade center in Zhangjiakou City failed to perform the Multi-level Protection Scheme requirement and its APP failed to protect personal information as required by applicable laws.

On October 27th, according to the laws and regulations such as *Cyber Security Law, PRC Telecom Regulation, The Rules on the Protection of Users' Personal information in Telecom and Internet Sector*, as well as the requirements under the *Notification of Commencement on the Governance of Infringement on Users' Rights and Interests through APPs,* MIIT has recently organized testing institutions to inspect mobile applications, and required that enterprises which have been found problems during the inspection to rectify the these problems. As of October 27th, 2020, 137 mobile applications still failed to complete the rectifications, including famous applications such as Xigua Input Method, Shanghai Disneyland and Guazi Car Market.

IV. Foreign Trends

On October 16th, the Information Commissioner's Office ("ICO") has fined British Airways ("BA") £20m for failing to protect the personal and financial details of more than 400,000 of its customers.

An ICO investigation found that the airline was processing a significant amount of personal data without adequate security measures in place. This failure broke data protection laws and, subsequently, BA was the subject of a cyber-attack during 2018, which it did not detect for more than two months.

ICO also stated that there were numerous measures BA could have used to mitigate or prevent the risk of an attacker being able to access the BA network. These include:

- limiting access to applications, data and tools only to those which are required to fulfil a user's role
- undertaking rigorous testing, in the form of simulating a cyber-attack, on the business' systems;
- protecting employee and third party accounts with multi-factor authentication.

About Llinks' Cyber Security and Data Compliance Services

Llinks' partners have been representing clients in data and cyber security related legal matters, such as offshore server, log records storage and filing, personal data collection and use, data integrity, centralized data process, differentiation between trade secrets and state secrets, etc. After 2010, Llinks' partners started to represent domestic and foreign enterprises in forming whole-process compliance solutions for the collection, use, transfer and destruction of customer personal information in digital marketing environment. In the course of handling these cases, Llinks' team has built up its solid capacity in tracing the logical chain which underlies all the data privacy laws and regulations. On that basis, our team can provide clients with practical and economical solutions which meet the requirements of the regulatory authorities.

Our team also includes some experienced lawyers who previously have served as law enforcement officials in cyber security administration. Their insights contribute to a better understanding on the regulatory authorities' key concerns and priorities in law enforcement, which is critically important for us to work out a practical solution for clients.

We have been working closely with relevant government consultancy departments and academic research institutions on the trend of legislation and implementation of the CSL regime. Our team has published special reports and analytical articles in this field, such as *Interpretation and Practice of the CSL*, *Practical Guidance on Trans-border Transmission Personal Information and Important Data*. In September 2018, LexisNexis published a special issue written by our team, on *Companies' Compliance in the Context of China*, which contains six articles on practical issues concerning cyber security and data compliance. In September 2018, we drafted a series of concise bilingual articles titled *30 Questions About the CSL*, which were later exclusively published online by Wolters Kluwer. Based on the latest legislation and practices, in 2019, we once again joined force with Wolters Kluwer to systematically update *30 Questions About the CSL* and publish the updated version titled *The Blue Book of PRC Cybersecurity and Data Compliance (Bilingual Version)*.

For more information, please contact:

David Pan Lawyer
Mob: +86 136 2172 0830
Tel: +86 21 3135 8701
david.pan@llinkslaw.com

Kenneth Kong Lawyer
Mob: +86 185 1210 5880
Tel: +86 21 3135 8777
kenneth.kong@llinkslaw.com

Xun Yang
Mob: +86 152 2182 2373
Tel: +86 21 3135 8799
xun.yang@llinkslaw.com

Patrick Gu Lawyer
Mob: +86 188 1746 8818
Tel: +86 21 3135 8722
patrick.gu@llinkslaw.com

Nigel Zhu Lawyer

Jianqi Yang Lawyer

Susan Deng