

# Personal data protection amid coronavirus

## Key takeaways for businesses operating in China

February 2020

### Outbreak of the coronavirus and personal data privacy

The fast-spreading coronavirus (Covid-19) has infected thousands of people in China and in over 20 other countries. This coronavirus outbreak, originating in Wuhan, a large city located in the central region of China, has been declared a Public Health Emergency of International Concern (PHEIC) by the World Health Organization.

In fighting against the outbreak of this new coronavirus, Chinese authorities at all levels have, in addition to providing emergency medical support to those affected by the virus, imposed quarantines and restricted travel and outdoor activities. In order to control the outbreak and track the spread of the virus, Chinese health authorities and other stakeholders ranging from airlines, rail operators and property management companies have collected a large amount of personal data, including data on individuals who have recently travelled to Wuhan or who have been in contact with those who have developed symptoms of infection. There have been several data breach incidents which have given rise to concerns over privacy and potential discrimination against people from Wuhan and Hubei Province.

In response to these concerns, the National Health Commission of China issued a notice on February 3, 2020 outlining the personal data protection requirements in the context of the prevention and control of Covid-19. In addition, on February 4, 2020, the PRC Cyberspace Administration of China (CAC) (the key Chinese regulator on cybersecurity and data privacy) issued the *"Circular on Ensuring Effective Personal Information Protection and Utilization of Big Data to Support Joint Efforts for Epidemic Prevention and Control"* (CAC Circular) to provide detailed guidance on protecting personal data in the current circumstances.

### Highlights of the CAC Circular

- The CAC Circular emphasizes the importance of protecting personal data in accordance with Chinese laws and regulations governing cybersecurity and the prevention of public health emergencies. Unless otherwise authorized under those laws and regulations, no individual or entity may collect or use personal data, without the consent of the data subjects.
- Where personal data is collected and used for the prevention and control of epidemic diseases, organizations that collect such personal data must adhere to the Personal Data Specifications (being the non-mandatory industry standards for data protection). The principles of necessity and minimum collection should be followed (for example, the data collected should be limited to those who are confirmed or suspected of carrying Covid-19 and those who have had close contact with confirmed or suspected virus carriers).
- Personal data collected for the purpose of preventing or treating epidemic diseases cannot be used for any other purpose. No personal information that has been collected for such use can be made public without the consent of the data subjects, unless this is necessary for the prevention of an epidemic and the information is redacted or anonymized.
- Companies that collect and control personal data must have strict technical and management measures in place to prevent data breaches.
- Companies with big data expertise and capabilities are encouraged to work with the government to use big data for the prevention and control of diseases.
- Non-compliance with Chinese laws and regulations in relation to the collection and use of personal data is subject to administrative sanctions, civil liability and even criminal penalties in case of severe violation. Individuals and entities are encouraged to report any breaches to the network regulators and the police.

## **Key takeaways for businesses operating in China**

The CAC Circular has important implications, notwithstanding that it was issued in the context of the prevention and control of Covid-19. Local and multinational businesses should take note of the following when handling personal data in China:

- It is obviously necessary to comply with Chinese data laws and regulations. Compliance with applicable laws and regulations is strictly enforced without exception, even for emergency situations.
- Although the China Cybersecurity Law does not make any exception for consent, the CAC has shown its willingness to refer to the non-mandatory Personal Data Specifications to accommodate specific scenarios where prior consent may not always be necessary or practically possible.
- Collection of personal data must follow the principles of necessity and minimization, and businesses must take proper technical measures (such as encryption) to prevent a data breach.
- Technology or big data companies which engage in collecting or processing personal data for the prevention and control of Covid-19, are required to obtain the consent of the relevant data subjects if they wish to use such data for research, market monitoring or for the development of new products or services.

## **Conclusion**

With the general public's increasing awareness of data privacy rights in China, Chinese authorities have taken enhanced actions to clamp down on businesses that fail to comply with Chinese data laws and regulations. We expect the Government will continue this approach. It is extremely important therefore that businesses take compliance seriously. Only then will they minimize regulatory risk and maintain general public trust in their products and services.

## **How we can help?**

Our global teams are actively advising clients in relation to the Covid-19 outbreak. Please do not hesitate to get in touch with your Norton Rose Fulbright client contact if your business has been affected.

---

**Contacts**

**Barbara Li**

**Partner**

Tel +86 10 6535 3130

[barbara.li@nortonrosefulbright.com](mailto:barbara.li@nortonrosefulbright.com)

**Bohua Yao**

**Associate**

Tel +86 10 6535 3169

[bohua.yao@nortonrosefulbright.com](mailto:bohua.yao@nortonrosefulbright.com)

The logo for Norton Rose Fulbright, featuring a small red triangle above the text "NORTON ROSE FULBRIGHT" in red, uppercase letters.

**NORTON ROSE FULBRIGHT**

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 4000 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, the Middle East and Africa.

**Law around the world**

[nortonrosefulbright.com](http://nortonrosefulbright.com)

Norton Rose Fulbright Verein, a Swiss verein, helps coordinate the activities of Norton Rose Fulbright members but does not itself provide legal services to clients. Norton Rose Fulbright has offices in more than 50 cities worldwide, including London, Houston, New York, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg. For more information, see [nortonrosefulbright.com/legal-notices](http://nortonrosefulbright.com/legal-notices). The purpose of this communication is to provide information as to developments in the law. It does not contain a full analysis of the law nor does it constitute an opinion of any Norton Rose Fulbright entity on the points of law discussed. You must take specific legal advice on any particular matter which concerns you. If you require any advice or further information, please speak to your usual contact at Norton Rose Fulbright.

© Norton Rose Fulbright LLP Extracts may be copied provided their source is acknowledged.  
EMEA22534 – 03/20