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

February 2020

On Enterprises' Obligations of Reporting Employees' Information during the Epidemic

By David Pan | Susan Deng | Emily Hu

After the outbreak of Novel Coronavirus Pneumonia (COVID-19), government departments, enterprises and institutions across the country have been actively collecting information on the epidemic situation with a view to maintaining the normal production order and economic order. On February 4, the Office of the Central Cyberspace Affairs Commission ("CAC") issued the *Notice on Protecting Personal Information and Using Big Data to Support Joint Prevention and Control* (hereinafter referred to as the "Notice"), which is intended to urge all local government departments and all institutions and entities to collect and report personal information related to the joint prevention and control of the epidemic situation in accordance with the law, to safeguard personal information security, and to protect personal privacy from any violation. In this special period, enterprises must not only make an orderly labor arrangement despite the impact by the epidemic, cooperate with the information reporting tasks, but also pay attention to employees' personal information and privacy protection. This article aims to clarify the legal basis for collecting and reporting employees' personal information to government agencies during this epidemic situation, and to further provide enterprises with some compliance tips on how to properly respond to requests for employees' information from government departments and secure employees' personal information and privacy at the same time.

For more Llinks publications, please contact:

Publication@llinkslaw.com

I. Rights and Obligations of Enterprises to Collect Epidemic Related Information

1. Enterprises are entitled to know the relevant information of employees for the purpose of arranging employees and restoring normal production and operation as soon as possible. According to Article 8 of the *Labor Contract Law*, enterprises "have the right to know the basic conditions of the employees directly related to the labor contract". During the critical period of epidemic prevention and control, if any employee has been infected or has a chance to be infected, it may threaten the health and safety of other employees in the office; for service industries where employees are extensively exposed to the population, it will even put the general public in danger, and thus cause an adverse impact on the company's normal operation as well as its goodwill. Based on this, enterprises are entitled to ask for information such as the travel records and health status of employees and their close contacts from employees (see the analysis below for the specific information that can be collected), because such personal information constitutes information that "directly related to the labor contract".

2. According to Article 12 and Article 31 of the *Law on Prevention and Treatment of Infectious Diseases* (hereinafter referred to as the "LPTID") and Article 21 of the *Regulation on Emergency Responses to Public Health Emergencies* (hereinafter referred to as the "Regulation"), every institution or individual is obliged to cooperate with relevant state organs in the prevention and control of epidemic; when patients with infectious diseases or suspected patients are found, such information shall be reported to disease prevention and control institutions or medical institutions in a timely manner, and no information about the epidemic situation shall be concealed, deferred or misreported. The foregoing regulations put forward statutory requirements for enterprises and individual employees to cooperate with relevant government departments in truthfully reporting epidemic information.

   Moreover, in accordance with Articles 10, 11 and 31 of the Regulation, based on the contingency plan for a national emergency prepared by the State Council, the local people's governments of provinces, autonomous regions and province-level municipalities shall formulate local contingency plan for their respective administrative areas, taking into account specific local conditions; such plan shall include the collection, analysis, reporting, and notification systems of information related to the emergency; the relevant local government departments should act according to the plan and undertake respective duties and responsibilities, which include collecting and reporting relevant information related to the epidemic. The provisions here grant relevant government departments with the authority and duties to collect, analyze, report and publicize epidemic related information during this certain period.

   Based on the above regulations related to epidemic prevention and control, government agencies in Beijing, Guangdong, Shanghai, Jiangsu, Zhejiang and other places have issued notices, instructions and guidelines requiring enterprises to assume the critical responsibility in epidemic prevention and control work, and to cooperate with the government. Such responsibilities include closely monitoring health status of the employees; collecting employees' recent health status, travel history to the places where the epidemic broke out before employees return to work; and reporting any abnormal situations in a timely manner.

In summary, the disease prevention and control institutions and medical institutions are mainly in charge of collecting epidemic related information, while the enterprises are merely obliged to cooperate with the aforementioned epidemic prevention and control work, and to collect and report employees' information to the relevant authorities. Enterprises should fulfil their legal obligations and assume social responsibilities in accordance with the specific requirements given by the local government on epidemic prevention and control and relevant information collection.

II. Compliance Tips on Information Reporting by Enterprises

1. Obtain informed consent from employees

Regarding the principles for the collection and use of personal information, the *Cybersecurity Law* has provided clear guidance, that is, "abide by the 'lawful, justifiable and necessary' principles to collect and use personal information by announcing rules for collection and use, expressly notifying the purpose, methods and scope of such collection and use, and obtain the consent of the person whose personal information is to be collected''. Article 8 of the *Labor Contract Law* gives the enterprise legal basis for collecting and using relevant employee information for making production and business arrangements, and clarifies the scope of information that can be collected, however, it does not exempt the enterprise from the above obligations of "due notification" and "obtaining consent". The Notice of CAC also clearly states that "except for institutions authorized by the State Council's health department in accordance with the *Cybersecurity Law*, the LPTID and the Regulation, no other institution or individual may collect or use personal information on the grounds of epidemic prevention and control without the consent of the person whose information is to be collected or used". This means that, if an enterprise intends to collect or use the personal information of employees beyond the purpose and scope of the aforementioned statutory information collection and reporting obligations, the enterprise shall obtain informed consent in advance. Considering that the enterprise needs to collect more information from employees for restoring normal business than required by the authorities out of epidemic prevention and control purposes, also considering frequent cyber violence cases of personal information leakage and privacy invasion, it is recommended that enterprises shall inform employees in a proper manner of the scope and purpose of collecting their personal information and obtain informed consent.

2. Stick to the "minimum and necessary principles" though out the full cycle of personal information processing, which starts with "collection", "use" and "disclosure" and ends in "storage and/or destruction".

Collection: Regarding the collection of employees' personal information, its scope shall be limited to realizing the purpose of joint prevention and control as stipulated in the LPTID, the Regulation and other laws and regulations, and follow the "lawful, justifiable and necessary" principles of the *Cybersecurity Law*. Personal information not related to epidemic prevention and control shall not be collected. Specifically, enterprises should "adhere to the principle of minimum scope; and in principle, the collection objects should be limited to key groups of people such as the diagnosed, the suspected and their close contacts",[1] and the information collected should also be limited to the necessary

[1] *Notice on Personal Information and Using Big Data to Support Joint Prevention and Control*: Collecting personal

scope which is "relevant to the epidemic" such as contact information, travel history within 14 days, contact history within 14 days, current physical condition, close contacts. The collection scope of personal information for other employees should be further limited and reflect the principle of necessity, for instance, only collect the location before return, return time, travel history in the severely infected areas, and avoid collecting travel and transport information, family relationships, medical examination reports and other irrelevant information. In addition, it would be better to adopt the "passive collection method", i.e. ask "yes/no" questions, rather than require employees to fill all information in the blanks, which can minimize employees' resistance and negative feelings.

Use: The Notice provides that "personal information collected for epidemic prevention and control shall not be used for other purposes." Therefore, enterprise shall use personal information exclusively for the purpose stated upon collection, which shall be clearly and strictly limited to epidemic prevention and control or employment management and business arrangements. The use of personal information must not exceed the legal limit or the scope of consent of the information subject. The personal information can neither be used for other purposes nor be used in combination with the information collected from other sources. However, it is worth noting that the Notice mentioned "encouraging capable enterprises to actively use big data under the government guidance, to analyze and predict the movement of key population such as the diagnosed, the suspects and their close contacts, as well as to provide big data support for joint prevention and control". The major information processed and used here should be anonymized information that reflects the group status only.

Disclosure: According to Article 42 of the *Cybersecurity Law*, enterprises shall not provide personal information collected to any third party without prior consent of the information subject; Article 12 and Article 68 of the LPTID also stipulates that information relating to personal privacy of patients infected, pathogen carriers, suspected patients, or persons in close contact with such patients shall not be purposely divulged. Based on the above regulations, the Notice requires that, except for the desensitized information which is required for the joint prevention and control, no entity or individual should not disclose personal information such as name, age, ID number, phone number, home address, etc. without the prior consent of the information subject. Therefore, enterprises should ensure that the personal information of employees is only provided to the relevant government agencies responsible for epidemic prevention and control; or that the relevant desensitized information is publicized to the public in accordance with the local contingency plan.

Storage and/or destruction: When the epidemic is over, enterprises should delete (or anonymize) the relevant personal information that no longer needs to be kept, unless otherwise required by laws and regulations.

3. **Safeguard personal information.** In response to the frequent divulgence of a large amount of personal information of the returnees and the diagnosed, local public security organs have cracked down on several personal information divulgence cases. Public security organs in Inner Mongolia,

information necessary for joint prevention and control should… adhere to the principle of minimum scope; and in principle, the collection objects should be limited to key groups of people such as the diagnosed, the suspected and their close contacts. In general, do not target the entire population in a specific area to prevent de facto discrimination against specific geographical groups.

Shanxi, Jiangsu and other provinces have imposed administrative detention penalties on information leakers[2]. In these cases, most personal information was leaked due to relevant person's mishandling when they were doing their job to sort out epidemic information within the company and forwarded relevant information to outsiders by screenshots; or by improper management decisions to disclose relevant employee information to everyone inside the company. As the process of reporting employees' information involves collection, statistical summary and disclosure, enterprises should pay close attention to the security of personal information in the whole process. Companies shall safeguard personal information in each step, take high-standard management and technical measures, in order to ensure the security of the personal information collected and prevent divulgence, loss or abuse of information. The specific measures that can be taken are as follows:

a) Arrange for specific personnel to concentrate on handling employees' information related to epidemic prevention, and expressly require them to keep such personal information known during the process strictly confidential, and not to illegally disclose, sell or provide it to others.

b) Limit the scope of the specific personnel involved, effectively implement the responsibility system with clear message delivered to them. For key employees in "close contact with the source of infection" who need to be directly contacted, a specific person should also be assigned to ensure that relevant contact information not to be spread. Also, information given to the such person should be limited to the "need-to-know" basis.

c) Store the personal information collected in a specific terminal device (preferably limited in the enterprise's intranet), encrypt it and adopt strict safeguard measures such as access restrictions and data audits.

d) Only report relevant information to the competent government agencies in strict accordance with the LPTID, the Regulation and the local government's contingency plan. When necessary, require the agency's contact officer to provide written evidence or authority, such as internal communication records, regulatory documents with official seals, etc.

e) Record and archive the information reported to government agencies, and specify the name of the receiving agency and the report time. While giving out information, request the recipient to safeguard the information in equal measures and keep a written record of the request.

Concerned with the trend of the epidemic, the government, enterprises and employees all hope that the epidemic would end, and the normal operation of social life would be restored as soon as possible. When collecting, using and reporting personal information of employees related to epidemic prevention and control, enterprises should meticulously balance its obligations out of public interest protection, corporate perception maintenance, government relations and the employees' legal rights.

[2] *Massive personal information related to the epidemic was divulged, and two local public security agencies made administrative detention penalties*: https://baijiahao.baidu.com/s?id=1657662679824821690&wfr=spider&for=pc

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

David Pan
+86 21 3135 8701
david.pan@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