大成 DENTONS

Practice/Industry sector: Competition and Antitrust/Privacy and Cybersecurity

Grow | Protect | Operate | Finance

Sort date: 2021.11.16

From the first outbreak of COVID-19 at the end of 2019 till now, the prevention and control of COVID-19 become a part of our daily life. In the workplace, enterprises may have to collect employees' sensitive personal information, such as vaccination status, results of COVID-19 test, places they have been to recently, etc.

However, employees have concerns over the safety and privacy of their personal information, which has become a hot issue especially after several cases where the individuals suffer from cyber violence because of the leakage of their personal information collected for the purpose of epidemic prevention.

The Personal Information Protection Law effective from 1 November 2021 emphasises the importance of the personal information protection and also provides guidance to both the employers and employees on how personal information should be collected, stored, transferred and utilized.

Of course, if an enterprise violates the applicable PRC data protection law when processing employees' personal information, an administrative fine up to RMB 50 million or 5% of the revenue of the previous year, suspension of business or even revocation of business license could be imposed on the relevant enterprise.

The directly responsible individuals may be subject to an administrative fine up to RMB 1 million and disqualification from being a director, supervisor, senior management, and chief personal information protection officer within certain period.

Given the above, we can tell appropriately and legally processing the employees' personal information is getting increasingly important. We hereby summarise from our past cases below the questions most concerned by our clients and our comments under the newly Personal Information Protection Law for you reference.

A. Can an enterprise require its employees to disclose their vaccination status, COVID-19 test results and places have been?

In general, yes, but with the employee's explicit prior consent.

Any information indicating the health condition and whereabouts of an individual is considered the individual's (sensitive) personal information and is therefore subject to data protection laws. With the exception of institutions authorised by the National Health Commission of China ("NHC"), no entity or individual has the right to collect, disclose or use personal information, unless the individual to whom the information relates provides their express consent (preferably in writing).

When requesting for the employees' consent, an employer should disclose to the relevant employee the details about collection, storage, usage, provision and disclosure of the personal information ("Information Processing"), for instance, the purpose and method of processing, period of storage, relevant rights the employee enjoys under the data protection laws. Besides the above, since the information concerned under this scenario are sensitive personal information, the enterprise should also obtain a separate consent on such data and inform the necessity of intended Information Processing and its possible impact on rights and interests of the employee concerned.

Since an enterprise normally would collect and process the personal information from a number of employees at once, the enterprise may wish to establish an internal policy regarding the Information Processing, such policy should at least specify the purpose, method and scope of the Information Processing. However, when dealing with sensitive personal information, it is advisable to set a separate chapter in the policy regarding the sensitive personal information and/or establish a separate policy in this regard, to ensure that employees give consent on the premise of full knowledge and reasonable consideration of the consequences for their own rights and interests.

B. Once obtained, how should an enterprise process the above personal information of its employees?

i. Usage

Once employees express their consent and provide relevant information to their employer voluntarily, the enterprise could use such personal information only for the purpose approved by the relevant employee, in our case, for the purpose of preventing and controlling the spread of COVID-19 only.

ii. Storage

The storage of personal information should be limited to the shortest period necessary for the intended purpose. For instance, if the enterprise wants to make sure that none of its employees nor their close family members have been to any medium/high risk areas during the Golden Week holiday, such information should only be stored long enough for fulfilment of such purpose, for instance, until it has been confirmed that relevant employees have not been exposed to COVID-19 during the holiday. The enterprise should also be responsible for protecting the stored information from being unintentionally disclosed to or hacked by a third party and deleting that information after the usage purpose is achieved.

iii. Cross-border Transfer

Firstly, if an enterprise intends to transfer its employees' personal information abroad, it has to meet one of the following requirements in advance: (1) passing the security assessment organized by the national cyberspace authority, (2) passing the personal information protection certification conducted by a professional institution selected by the national cyberspace authority, (3) entering into a contract following the standard template provided by Cyber Administration of China with the overseas recipient, establishing the rights and obligations of both parties; or (4) other conditions provided by laws and regulations.

Secondly, prior to the cross-border transfer, the enterprise shall also conduct the personal information protection impact assessment on the relevant employees and prepare the corresponding information protection method. The assessment should at least cover (1) whether the purpose,

method, etc. of such transfer is lawful, legitimate and necessary, (2) the impact and potential risks on the person's rights and interests, and (3) whether the protection measure is legal, effective and match the level of risk. Such assessment report and records of cross-border transfer shall be kept for at least three years.

In addition to the above, a separate consent from the employees is still a necessity. It is also advisable to enter into an information protection agreement with recipient of such personal information stipulating that the recipient should protect the relevant personal information received at least at the same level provided in the PRC personal data protection laws.

C. Can an enterprise share such information to a third party, like its affiliates?

In general, yes, but with the employee's explicit prior consent.

As mentioned above, such information of an employee is subject to applicable data protection laws. Hence, if an enterprise wants to share such information obtained from its employees to its affiliates for the purpose of disease prevention and control, the employee's prior explicit consent is a must. To be specific, it is advisable for the enterprise to obtain the employee's consent for the purpose of sharing, use and specific recipients of such information in writing.

In such cases, the recipients should also follow the applicable data protection laws to ensure the confidentiality of the personal information disclosed to them.

Disease control and personal information protection can and should be achieved at the same time. When collecting its employees' personal information in an attempt to better prevent and control the spread of COVID-19 within its own capability, an enterprise should firstly obtain the prior written consent of the relevant employees when collecting their personal information, while providing explicit personal information processing policy and make sure the relevant employees have easy access to such policy.