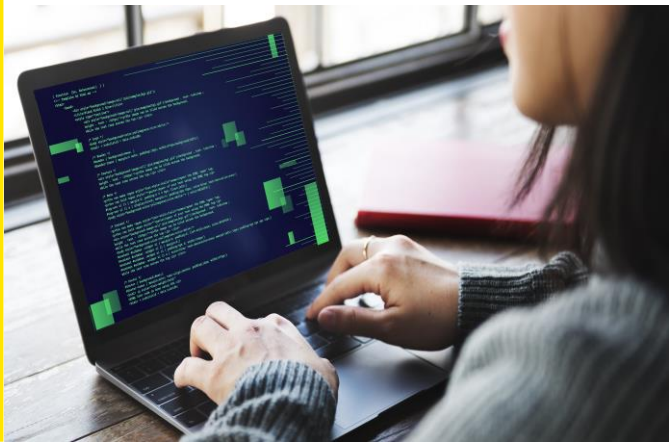
COVID-19: DATA PROTECTION RISKS AND MITIGATION STRATEGY

LC Lawyers
林朱律師事務所
Law firm member of the EY global network

10 April 2020 | **Kareena Teh**, **Philip Kwok**, **Catherine Wong**

We recommend that these protocols take into account the five key considerations



Many companies have been monitoring employees' personal and health data because of the COVID-19 outbreak. Others have been adopting flexible working arrangements to minimize the health risks associated with employees and customers being in close physical contact, resulting in millions of online interactions and transactions taking place. These activities have created additional data security risks that, if not properly managed, could result in breaches and consequential loss of reputation and business, regulatory enforcement actions and litigation.

In this article, we set out our recommended approach to managing the additional COVID-19 data security risks.

Designing data protection protocols to mitigate data security risks

The first step in designing a data protection protocol is to identify the types of data that are being collected, processed and used.

In the context of COVID-19, there are at least four types of collected data that need to be protected:

- **Personal data of employees**: This includes employees' name, employee ID, address, relatives, and location data.

- **Health data of employees**: This includes health data and health history of employees, such as collecting information as to whether the employee has specific symptoms.

- **Customers' personal and confidential data**: This includes customers' personal and confidential information, such as customers' name, identity card / passport number, work and residential address, email address, phone number, and bank account details.

- **Company's sensitive and confidential information:** This includes proprietary trade secrets, sensitive information that may be considered information of critical information infrastructure and/or state secrets under mainland China law, and all other sensitive and confidential information.

Once the types of data that are being collected, processed and used have been identified, it is advisable that companies develop dedicated confidentiality and security protocols or revisit the existing protocol to ensure mitigation of risks to data breaches arising out of the COVID-19 outbreak.

We recommend that these protocols take into account the five key considerations set out below.

Key consideration 1: Comply with personal data protection principles

The first area of paramount importance is to have protocols to ensure that your collection and processing of personal data complies with all applicable personal data protection principles.

From a Hong Kong perspective, compliance with the Personal Data (Privacy) Ordinance (**PDPO**) is key. These principles include, on a non-exhaustive basis:

- Making sure the personal data collected in a COVID-19 outbreak is **necessary**, **adequate** but not **excessive**.

- Making sure that the personal data collected is **accurate** and are **kept not longer than necessary** for the fulfillment of the purpose (including any directly related purpose) for which the data is or is to be used.

- Making sure that the data subject is **informed** of the purpose for the use of the data, and the classes of persons to whom the data may be transferred, usually by way of a personal data protection policy or personal data collection statement.

- Making sure **voluntary and express consent** is obtained from the data subject for any use of the data subject's data for a purpose not directly related to the purpose at the time the data is collected. In the COVID-19 context, there may be circumstances where it may be necessary to disclose personal information and/or health information of your employee without the employee's consent if, for example, your employee is a confirmed COVID-19 patient and/or a close contact of a COVID-19 patient. While there are exemptions for a consent requirement under, for example, section 59 of the PDPO if the disclosure is in the interests of preventing serious harm to the physical or mental health of the data subject or any individual, such exemptions have a strict ambit and any disclosure should be carefully considered.

- Making sure that you have readily accessible personal data collection statement and policy, which should provide for the collection and use of personal data in the COVID-19 context.

- Making sure that there are proper procedures in place for handling data access and data correction requests. It should be noted that there may be exemptions to compliance with data access requests (not data correction requests) where the situation falls under the Health exemption under section 59 of the PDPO, or Staff Planning under section 53 of the PDPO.

Key consideration 2: Implement confidentiality measures for work-from-home arrangements

The second area of equal importance is having protocols with confidentiality measures for your work from home employees to protect your company's sensitive and confidential information (which could include customer and employee data) which is now being accessed through a work from home environment that may not be as secure as an office environment, particularly if your

employees are living with and working in close proximity with other people who are not also your employees. Some additional precautionary measures to consider implementing include:

- Using mandatory privacy screen shields for laptops.
- Taking calls away from other people and where possible, in separate rooms.
- Using headsets for confidential calls.
- Making sure that hard copies of your company's confidential information are securely disposed of and/or kept after its use.

Key consideration 3: Implement data security measures

The third critical area which your protocols should address is having security measures for the protection of all kinds of data, including personal data, health data, customers' data, company's sensitive and proprietary data, etc. These measures should include considering the following issues:

- The technical measures in place to guard against unauthorized or accidental access, processing, use, erasure or loss of data, bearing in mind that in a work-from-home arrangement, employees are accessing your company's network without the security measures that are in place at the office.
- Appropriate data backup measures in place to guard against any accidental loss of data due to security issues or system breakdowns.
- Measures to guard against internet fraud, scams, phishing emails, etc., including verification procedures for verifying identities of requests for money transfers.
- Emergency and action plans for data breach.

Key consideration 4: Comply with cross-border data transfer laws and regulations

The fourth area which your protocols should cover is compliance with cross-border data transfer requirements, taking into account the jurisdictions where you are hosting the data and the jurisdictions to which the data is being transferred. Jurisdictions such as mainland China and Europe have particularly stringent data transfer requirements. Some key issues to consider and address are:

- Have cross-border transfers become or are they likely to become necessary and more prevalent due to the COVID-19-driven closure of borders and travel restrictions?
- Have you complied with all applicable foreign laws and regulations concerning cross-border data transfer? For example, have you considered the applicability of the personal data protection, processing and transfer rules under the European Union General Data Protection Regulations and complied with the same?
- Have you considered whether your company's services may be covered by and considered "critical information infrastructure" under the mainland China Cybersecurity Law, and if so, have you complied with the relevant regulations concerning cross-border data transfer?

- Have you considered whether you may be handling information and documents which may be categorised as state secrets, and is it permissible to take the relevant processes online in light of compliance with state secrecy provisions?

Key consideration 5: Comply with sector specific regulations

If your business is regulated, you will also need to ensure that your protocols comply with sector-specific regulations. Additionally, if you are turning to innovation as a means of overcoming and/or easing the disruption to the provision of your services during COVID-19, you need to be aware that specific regulations may apply to certain areas of services provided, including those involving non-face-to-face approaches to clients' businesses. Some key issues to consider for your protocols are:

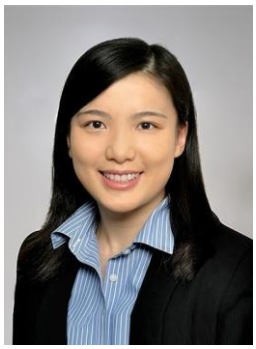
- Have you checked and complied with specific regulations concerning non-face-to-face approaches to client's businesses?

- Have you checked and complied with specific regulations concerning electronic signing of documents as well as other sector-specific regulations such as those concerning non-face-to-face identity verification?

KEY CONTACTS

Kareena Teh
Partner, LC Lawyers LLP
kareena.teh@eylaw.com.hk
+852 2629 3207

Philip Kwok
Counsel, LC Lawyers LLP
philip.kwok@eylaw.com.hk
+852 2675 2160



Catherine Wong
Associate, LC Lawyers LLP
catherine.ky.wong@eylaw.com.hk
+852 2675 2173

Contact us

LC Lawyers LLP *in Association with* Chen & Co. Law Firm
Suite 3106, 31/F, One Taikoo Place
979 King's Road, Quarry Bay
Hong Kong
Tel: +852 2629 3200
Fax: +852 2956 1980

https://www.eylaw.com.hk/en_hk

Follow us on WeChat