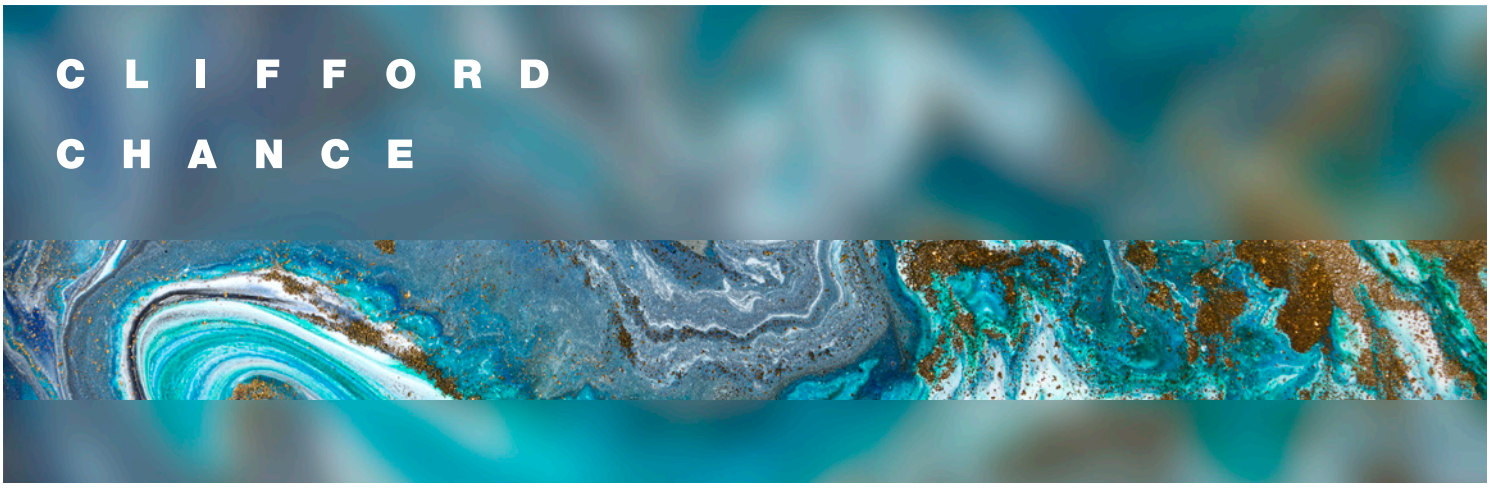

CORONAVIRUS: THE DATA PROTECTION CHALLENGES

As the Coronavirus outbreak continues to spread, companies are implementing an increasing number of measures to prevent contamination of their premises and amongst their staff. These measures sometimes require them to collect, analyse and share information about individuals, to comply with Health and Safety regulations, but it does raise data protection challenges. What types of personal data can be collected, and how? Can it be shared with group companies, and with entities outside the group such as service providers and authorities?

These questions emerge in the employer-employee relationship, but they also arise when dealing with other stakeholders who are in contact with the workplace, namely customers, contractors and other visitors.

This Q&A outlines some of the key steps to keep Coronavirus (Covid-19) containment in line with GDPR requirements (with respect to both employees and other stakeholders), and briefly addresses other privacy laws in different regions of the world. Of course, there is no valid "one-size-fits-all" approach under data protection law, so these steps should be adapted to the specificities of each contemplated Coronavirus-related measure.

Under the GDPR

Q: Does the GDPR allow companies to collect travel and health data for Coronavirus containment (e.g. information on recent travel, exposure to contaminated individuals, symptoms)?

Travel data can be collected provided the company complies with essential principles such as transparency, lawfulness and security. Health data collection is prohibited, but there are exceptions to that rule as explained below. Naturally, in crisis situations such as the Coronavirus pandemic, meeting GDPR requirements will be easier if ongoing compliance processes are already in place.[1]

Q: How do you lawfully collect such personal data under the GDPR?

Before collecting the data, the company should take the following steps:

- **Lawfulness:** the legal basis for using data should be identified on a case-by-case basis. In the Coronavirus containment context, the "legal obligation" basis – provided

1 As a reminder, companies outside the European Economic Area ("EEA") should not assume that they are outside the scope of the GDPR. Rather, they should proactively assess whether their data uses are caught by the GDPR's extraterritorial provisions (e.g. a US company requiring Coronavirus questionnaires to be completed by EEA employees via its establishment in France could be subject to the GDPR for this activity).

collecting data is necessary to comply with an EU or local European law – or "legitimate interests" will likely be considered appropriate legal bases. Conversely, the conditions for using "consent" or "vital interests" as legal bases would less likely be met;

- **Sensitive data:** GDPR broadly defines health data as any information related to an individual's physical or mental health. Therefore, health data not only covers information that is "obviously" health-related (such as a description of symptoms) but also more general information (e.g. where an individual is calling in sick). Before collecting any health information, the company must ensure it meets one of the conditions to handle sensitive data, in addition to the legal basis mentioned above. In particular:
  - In a work environment, the company should identify the EU or local European law – in the field of employment or public health – that permits the health data collection. For instance, that law may consist in an employer's legal obligation to ensure workers' health and safety, that justifies measures to limit the spread of the virus.
  - In certain circumstances (which would be rare), explicit consent may work.
- **Transparency:** individuals about whom personal data is collected should receive a privacy notice, before or at the moment of collection, that details the main characteristics of the data use. The company can either (a) update existing privacy notices if they do not cover disease containment or (b) create a new privacy notice dedicated to Coronavirus;
- **Data Protection Impact Assessment (DPIA):** given the nature of Coronavirus-related data processing activities – e.g. they may involve sensitive data and evaluation of health risks – a DPIA would likely be required under the GDPR, and, in this context, the related safeguards would have to be implemented.

Q: What personal data could be collected?

Companies should only collect necessary personal data. In the context of Coronavirus containment, this means collecting the minimum information (see below for more details) needed to evaluate the risk that an individual carries the virus and take proportionate, risk-based measures.

Data likely deemed necessary	Data unlikely deemed necessary
• Presence of Coronavirus symptoms • Confirmation as to whether the person recently traveled to "hot zones," which currently include China and other countries such as Italy, South Korea, Japan and Iran. Information can cover both professional and non-professional travel • Close contact with individuals who have recently been in "hot zones" and/or showing Coronavirus symptoms.	• The person's nationality • The identity of the individuals to whom that person has been exposed • Countries visited that are not "hot zones. Or countries visited before the incubation period.

Of course, what is considered as necessary information may evolve as scientists learn more about Coronavirus.

Q: How should personal data be collected?

In terms of data collection method, the least intrusive option should always be selected. This may require adopting a gradual, risk-based approach, such as:

1. Provide questionnaires with targeted yes / no questions to carry out a first screening of individuals' Coronavirus. Review the questionnaires to ensure only required information is collected. On the basis of the initial screening results, notify individuals presenting high contamination risks of the measures that will need to be taken to limit their interactions with the workplace;
2. Request individuals who provided incomplete or improperly completed questionnaires to confirm information.

Moreover, some organisations ask themselves whether they could implement or cause the implementation of medical tests (e.g. temperature scanning, blood tests). These would raise many issues from a GDPR standpoint (given the intrusiveness of such tests) and other perspectives (e.g. right to bodily integrity, doctor-patient confidentiality).

Q: Does the GDPR allow companies to outsource the collection and analysis of Coronavirus-related personal data?

Yes, provided this outsourcing does not reduce the level of data protection. In particular, the company should engage with service providers having the capacity to comply with GDPR obligations – as demonstrated by audit reports and labels – and formalise the relationship with an appropriate data protection agreement.

Q: Can a company share Coronavirus-related personal data with others?

Yes, if it is absolutely necessary (e.g. involvement of a contractor or a group company needed to implement sufficient health and safety measures) or mandatory (e.g. sharing of information with government agencies). In any case, such data sharing should take place in compliance with all GDPR requirements (e.g. determination of a legal basis, information of the concerned individuals, data minimisation, implementation of security measures, entering into appropriate data protection provisions).

For the sake of transparency, a company may inform its staff about the infection of others (e.g. employees, visitors), provided it does not communicate personal information (e.g. names, position of the infected individuals).

Beyond the GDPR

Q: What are the legal requirements beyond the GDPR?

Strict data protection laws – some of them GDPR-inspired – are being adopted all over the world. Companies taking Coronavirus measures in various jurisdictions should ensure they address local requirements. For example:

- **Local European laws:** European countries have often adopted stricter requirements than the GDPR in the fields of employment and health. A company should not assume that, by complying with the GDPR, it automatically complies with European local privacy laws.[2]

2 For instance, the French data protection authority (the CNIL) just indicated, in a publication dated 6 March 2020, that health data could be collected by organisations, only upon request from public authorities. See: https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles (in French).

- **Asia:**
  - **China:** The government of the People's Republic of China (PRC) has reinforced data protection requirements during the COVID-19 outbreak. Where a company is willing to process an individual's personal data (e.g. information on whether he/she (i) is infected, (ii) has been in direct contact with infected persons, (iii) recently travelled to or from certain cities in order to prevent and control COVID-19 expansion), it will need to obtain his/her prior consent. That said, a simple implied consent (i.e. asking an individual to provide relevant information before entering the workplace, and such individual voluntarily provides the requested information) may suffice. Moreover, companies will have to comply with PRC law principles of lawfulness, necessity and minimisation.
  - **Hong Kong:** A company may process an individual's identity, location and health-related data without collecting his/her consent, if processing the relevant data would be necessary to avoid causing serious physical or mental harm to individuals (this could be the case in the Coronavirus context).
  - **Singapore:** A company may collect, use and disclose an individual's personal data (e.g. identity, location and health-related data) without collecting his/her consent, provided that the contemplated processing is necessary to respond to an emergency that threatens the life, health or safety of other individuals (this could be the case in the Coronavirus context). In addition, the relevant company should ensure that it has security arrangements in place to protect the personal data at stake from unauthorised access or disclosure.
- **Australia:** Under the Australian Privacy Principles (APPs), sensitive information (which includes health information) is generally afforded a higher level of privacy protection than other types of personal information. Consent of the individual would likely be required if a company is to ask questions in relation to his/her health, in the Coronavirus context. Moreover, strict obligations would apply in respect of the use and disclosure of this sensitive information (including any disclosure to an overseas recipient).
- **United Arab Emirates (UAE):** The Dubai International Financial Centre (DIFC) financial free zone and the Abu Dhabi Global Market (ADGM) financial free zone have their own data protection regulations that apply to companies incorporated within those free zones. DIFC and ADGM's data protection requirements are similar to those provided for in the GDPR. In addition, consent of the individual would likely be needed if health-related data were to be disclosed by a company to third parties.

CONTACTS

Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova
@cliffordchance.com

Grégory Sroussi
Counsel
Paris
T: +33 1 4405 5248
E: gregory.sroussi
@cliffordchance.com

Chinwe Odimba-Chapman
Partner
London
T: +44 20 7006 2406
E: chinwe.odimba-chapman
@cliffordchance.com

Jonathan Kewley
Partner
London
T: +44 20 7006 3629
E: jonathan.kewley
@cliffordchance.com

Arun Visweswaran
Senior Associate
Dubai
T: +971 4503 2748
E: arun.visweswaran
@cliffordchance.com

Connor Partos
Associate
Dubai
T: +971 4503 2664
E: connor.partos
@cliffordchance.com

Ling Ho
Partner
Hong Kong
T: +852 2826 3479
E: ling.ho
@cliffordchance.com

Anita Lam
Senior Consultant, HK
Head of Employment
Hong Kong
T: +852 2825 8952
E: anita.lam
@cliffordchance.com

Kimi Liu
Counsel
Beijing
T: +86 10 6535 2263
E: kimi.liu
@cliffordchance.com

Lijun Chui
Counsel
Singapore
T: +65 6506 2752
E: lijun.chui
@cliffordchance.com

Tim Grave
Partner
Sydney
T: +61 2 8922 8028
E: tim.grave
@cliffordchance.com

Floris van de Bult
Co-Head Global
Employment Practice
Amsterdam
T: +31 20 711 9158
E: floris.vandebult
@cliffordchance.com

Sanne Blankestijn
Associate
Amsterdam
T: +31 20 711 9131
E: sanne.blankestijn
@cliffordchance.com

NOTES

OUR INTERNATIONAL NETWORK
32 OFFICES IN 21 COUNTRIES

Abu Dhabi
Amsterdam
Barcelona
Beijing
Brussels
Bucharest
Casablanca
Dubai
Düsseldorf
Frankfurt
Hong Kong
Istanbul
London
Luxembourg
Madrid
Milan
Moscow
Munich
Newcastle
New York
Paris
Perth
Prague
Rome
São Paulo
Seoul
Shanghai
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.

Riyadh*

*Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh
Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

2003-000099