Mexico - Data Privacy & COVID-19 Challenges

April 13, 2020

As the Coronavirus emergency state endures, companies are employing measures to prevent the outbreak and spread in their facilities. This six-point insight serves as a practical aid to in-inhouse counsel, privacy officers, and businesses that are addressing privacy challenges triggered by COVID-19.

1. In the context of COVID-19 and the Federal Data Protection Held by Private Parties Law, companies should only collect and process essential data. It is about being **proportionate**.

Likely Proportionate	Likely Unproportionate
Health (information on symptoms and testing) data for COVID-19 containment	Nationality
Travel (information on risk-zones travel) data for COVID-19 containment	Gender
Close contact with individuals who have recently been diagnosed with symptoms or traveled to countries deemed as unsafe	Third-party identity to whom that person has been exposed.

2. Before collecting the data, the company should ensure **transparency.** Employees, visitors, costumers, and in general all individuals should receive a privacy notice that covers health data, before or at the moment of collection. The privacy notice must explicitly specify that it handles sensitive data.
3. In the COVID-19 context, a business may perform to its customers, visitors and employees a symptom/temperature safety assessment or full RT-PCR testing. Companies may also share this information with labs, health authorities, and other third parties. As a rule, express **consent** is necessary to lawfully collect, process and share sensitive (health) data. In certain circumstances (exceptions), a company could carry on without consent.
4. The employment of measures such as pseudonymization (replacing personally identifiable material with artificial identifiers) and encryption (encoding messages so only those authorized can read them) is highly recommended to preserve an **expectation of privacy**.
5. There is no “one-size-fits-all” action when complying with the **responsibility** principle. Companies should take active steps (e.g. implement security systems and storage infrastructure used for the processing of health data; conduct Security Measures gap analysis, provide appropriate training to Data Controller’s officers involved in the data processing activities, etc.) to comply.
6. In terms of the **quality**, **loyalty** and **purpose**principles: COVID-19 data should be collected in the least intrusive approach possible. Health data should only be processed and shared for the purposes previously informed in the privacy notice. Health data should be securely erased when it is no longer needed in terms of the privacy notice. As a good practice, we suggest employers avoid intrusive questionnaires and create inter-company awareness of the COVID-19 symptoms; thus, encourage employees to voluntarily disclose health or travel information.

INAI Guidance

The National Institute of Transparency, Access to Information and Protection of Personal Data (INAI) has published (see here) helpful guidance on the above mentioned and:

- Privacy Rights Requests.
- Recommendations on the Processing of Sensitive Data.
- Frequently Asked Questions on Data Privacy and COVID-19

We will provide further guidance as the COVID-19 pandemic continues to evolve in Mexico. To ensure you do not miss any updates or if you require support, please contact us.

Your Key Contacts

Sergio Legorreta
Partner, Mexico City
D +52 55 1010 9843
sergio.legorreta@dentons.com

Amanda Valdez
Partner, Mexico City
D +52 55 3685 3313
amanda.valdez@dentons.com

Rogelio Lopez-Velarde
Partner, Mexico City
D +52 55 3685 3334
rogelio.lopezvelarde@dentons.com