COVID-19 and personal data processing 1/15/20

Due to the emergency situation declared in Latvia for COVID-19 containment, companies as well as central and local government agencies have taken measures to protect their workers, customers and other persons against potential threats to their health in order to continue working to the extent possible in the emergency situation. Under the circumstances, a new type of information about individuals is additionally being gathered and processed, for example, whether they have any symptoms, whether the person has been in contact with anyone who might be infected, including any COVID-19 tests and their results, as well as other information relating to places someone has visited.

The information being gathered by companies is personal data, including special categories of data, about identifiable individuals, and this data processing is subject to tight requirements under the General Data Protection Regulation (GDPR). This article explores key issues that companies should bear in mind when it comes to processing personal data for the detection and containment of COVID-19.

Matters that must be considered

First of all, the information being gathered from individuals in relation to COVID-19 is basically considered a special category of data because article 9(1) of GDPR treats data about an individual's health as a special category.

Given the ongoing emergency in Latvia and globally, when it comes to attempts at containing COVID-19, companies are permitted to process personal health data but must ensure that data subjects (individuals) are notified in line with GDPR. This is because under the circumstances, companies may gather information that was never obtained before and is not directly related to their business, but the current basis for obtaining such information from individuals is COVID-19. For example, a company may additionally gather information on whether its workers are constantly isolated, information about the body temperature of workers and visitors, and any other information the company is able to represent as related to containing COVID-19 and safeguarding the life and health of other individuals.

The processing of personal data, in particular special categories of data, is governed by tight requirements under GDPR and national rules. Once a company as a personal data processing controller obtains information about individuals, the company is fully responsible for its lawful processing according to GDPR requirements.

Secondly, the company needs to understand and clearly define what personal data and what special categories of data it obtains from individuals according to its purposes and goals set by the Latvian government to contain COVID-19. Otherwise the company might be obtaining too much personal data, which may be illegal even in the present circumstances. GDPR makes it clear that only so much information about the individual may be obtained as is absolutely necessary for achieving the company's stated aim.

Before gathering any data from individuals, the company should have a clear goal and understanding of what personal data and what special categories of data are necessary for achieving its stated aim, which is basically COVID-19 containment.

For example, if the company decides that a worker must be staying isolated at home, it may be sufficient to ask questions about whether the person or any other household member has any COVID-19 symptoms

(as opposed to asking for small and specific details).

Taking this approach will ensure the company follows the GDPR data minimisation principle and does not store any unnecessary information about its workers, which might pose a significant risk of breaching GDPR. At the same time, the company must ensure that any information about individuals obtained during the COVID-19 containment period is stored only for so long as there is a purpose for processing that personal data.

Thirdly, the company must have an adequate lawful basis for processing personal data obtained due to COVID-19. Under GDPR if the company is to have a lawful basis for personal data processing in the context of COVID-19, the company can rely on the following bases for legal data processing:

- *Legitimate interests.* The company may consider it necessary to process personal data about a worker and other related individuals to secure the company's legitimate interests in maintaining business continuity and carrying out its obligations towards individuals who are directly dependent on its ability to provide, for example, jobs or services to customers. The company needs to figure out whether its own interests in personal data processing override the interests, rights and fundamental freedoms of those persons. So it is advisable to run an interest balancing test related to this type of personal data processing the company is or plans to be doing.
- *Contractual performance.* If personal data processing related to COVID-19 is necessary to enable the company to honour its obligations towards workers under their employment contracts (whether express or implied terms), for example, an obligation to ensure the health, safety and wellbeing of workers, then such processing may be based on contractual performance.
- *Statutory obligation.* Depending on applicable legislation, the company may have statutory obligations for health and safety, and it is possible that an external statutory instrument requires the company to carry out some specific personal data processing activities that may be based on the company's statutory obligation.

However, although the company may have a lawful basis for processing such personal data, this is subject to the obligations the company has as a controller under GDPR, for example, the duty of notification and the implementation of adequate technical and organisational measures, which have not been cancelled during the period the world is struggling to contain COVID-19. Even if the supervisory authority turns a blind eye to potential data processing breaches at the moment, the company should expect that if the National Data Office finds that data processing was unlawful or GDPR requirements were not met in data processing, the Office will impose a penalty at a later date after the breach was committed or detected, so companies should not expect that any potential data protection breaches committed during the emergency situation will go unpunished if detected later.

The company's obligations

It is clear that companies are currently facing other problems, and personal data processing might be the last thing to bother about. However, to avoid running into new problems once the COVID-19 crisis is over, there are certain things that companies using remaining workers can do at the moment to ensure that personal data processing done for the purpose of containing COVID-19 and coping with its consequences is lawful.

The company is also advised to take this opportunity for revising and updating its privacy statements if

necessary. Revising existing privacy statements is crucial to make sure they offer the necessary information about the data obtained and explain the purposes the data is processed for. If the company gathers some new personal data or special categories of data from individuals and uses it for a new purpose, the company might have to update its privacy statements to reflect the changes to how it gathers data from individuals.

From a data protection compliance perspective, companies should also consider a number of other issues, including the disclosure of COVID-19 cases to other workers. As part of the company's obligation to ensure workers' health and safety, employers can inform their employees of COVID-19 cases according to statutory requirements. Such disclosures must be limited as far as possible. If it is necessary to disclose the name of a worker who, for instance, has been diagnosed with COVID-19 (and this is otherwise permitted under applicable legislation) to enable other workers to take adequate protection measures, the worker whose data is to be disclosed must first be informed of the intended disclosure, while at the same time ensuring that the worker's data is disclosed neither excessively nor to anyone who is not supposed to have this information.

If the company receives a data subject's request but all of the company's thoughts and efforts are focused on coping with the consequences of COVID-19, the company should nevertheless take care to meet deadlines for replying to the data subject's request. If the company is concerned that it might be unable to meet the GDPR deadlines, the company should inform the data subject as soon as possible that a reply to their request will be prepared as soon as reasonably practicable but under the circumstances it cannot be given by the stated deadline.

The company should consider conducting a data protection impact assessment because article 35 of GDPR prescribes it as mandatory where specific data processing activities are carried out. GDPR requires the company to conduct an impact assessment if processing might pose a major risk to personal rights and freedoms. The impact assessment is designed to help the company figure out what risks are associated with specific data processing activities and what measures the company can take to mitigate those risks. The impact assessment will also help disclose any necessary changes in the company's other compliance documents concerned with data protection (such as the privacy statement and the record of processing activities).

Things worth considering

Under the circumstances, it will be crucial for companies to carefully monitor the security of their systems and cyberthreats. Personal data and special categories of data should be properly protected and, in particular with respect to health data being processed, security measures to protect such data should be more stringently applied. Companies must also make sure they continue to meet deadlines for notifying the supervisory authorities (and any private persons if necessary) about personal data breaches if the breach is so serious that it attracts the duty of notification under GDPR.

At the same time, we recommend assessing whether your company needs to enter into data processing agreements with third parties (such as IT service providers or health care providers).

The supervisory authorities appreciate that companies may find it hard to meet all the data protection compliance standards with their resources being allocated for the containment of COVID-19. Some of those supervisory authorities have said that no sanctions should be imposed on companies that are currently unable to perform their obligations. Of course, this is a welcome move, yet this seeming flexibility should be interpreted very narrowly. Companies should continue to follow the guidelines issued for meeting data

protection requirements and carrying out instructions of the national data protection supervisory authorities in countries where the company operates.