Client Alert

April 2020

Key Data Protection Considerations Related to COVID-19 in the EU

Where Do We Stand?

As businesses continue to face unprecedented challenges resulting from the COVID-19 pandemic, ensuring individuals' safety and the survival of business are two goals that are at the top of companies' priority lists. To facilitate these goals, there are a number of key data protection considerations that companies doing business in the EU should take into account.

Data Protection Considerations in the Fight Against the Virus

In the first days and weeks following the COVID-19 outbreak, the immediate focus of businesses and regulators was on legal questions regarding the lawfulness of collecting and sharing certain types of personal data to try to slow down the spread of the virus and ensure health and safety in the workplace. Specifically, these questions involved the lawfulness of:

- Processing the health information of company employees and visitors, for example, in connection with conducting temperature tests and through surveys regarding health status, visits to high-risk areas and contact with infected individuals;
- Revealing the identity of infected individuals in the workplace to colleagues and authorities;
- Processing employees' personal contact details, such as mobile phone numbers, for emergency communications; and
- Processing location data to track potential exposure to the virus.

Businesses should consider these questions as regulatory guidance continues to evolve. These issues also may continue to be relevant in the post-lockdown era.

Data Protection Considerations Related to Business Continuity

Recently, businesses and regulators have shifted their focus toward data protection considerations related to confinement measures in response to the COVID-19 situation and ensuring the business continuity of privacy compliance programs. In this regard, businesses should consider:

- Updating the company's cybersecurity framework to ensure appropriate data security, resilience of systems, availability of resources and effective response in the event of cyberattacks;
- Implementing measures for long-term safe teleworking, issuing data protection-related guidelines and organizing trainings to make employees aware of data security risks; and
- Identifying key vendors and managing and reviewing vendor agreements.

From an operational perspective, it is important to limit disruptions and delays in business operations while the COVID-19 situation lasts. To that end, issues to consider include:

- Who to contact for data protection reviews of products and services if key individuals or the data protection officer becomes unavailable;
- How data protection impact assessments about crisis measures will be conducted and, if required, how high-risk privacy matters will be escalated internally; and
- How data subject rights requests will be handled if key individuals are not physically present at the workplace.

Contacts

David Dumont
ddumont@HuntonAK.com

Anna Pateraki
apateraki@HuntonAK.com