Contact tracing

Leveraging technology to create a safer environment

Unprecedented impact on society and organisations around the world

COVID-19 has triggered risks for which society and organisations weren't prepared. The speed with which risks associated with the pandemic have emerged is unprecedented. Society and business as we knew it have been destabilised and everyone's looking back with disbelief on what's just struck our world.

After the initial outbreak of COVID-19 and the lockdowns that followed, we're now about to face the next challenge: gradual deconfinement, with workers in non-essential services beginning to return to their jobs. This return to work is being accompanied by protection measures such as the distribution of millions of face masks and a major escalation in testing programmes. Organisations need to gear up to cope with the long-lasting impact of COVID-19 and create a safer work environment for employees who'll soon start returning to their professional work environment.

83%

Don't have systems and processes in place to track of their workforce

Building a future-proof and safer work environment

With people gradually returning to their regular activities and work environments, attention's now focused on tracing the path of corona infections, and the use of personal data linked to contamination and immunity, to contain the progression of the virus and prevent new waves of infection.

Maintaining a strong connection with your workforce is paramount to maintaining employee confidence and productivity in times of disruption. The ability to obtain the information needed to better protect your workforce, mitigate business risks and build confidence around returning to work is becoming a new standard of workforce management.

Privacy

Our data protection laws are well-equipped to help support public safety and aren't an obstacle to tracking the virus, a variety of mobile apps that do just that are already springing up. Times of change and uncertainty shouldn't prevent you from operating based on your values, in line with applicable laws and regulations, including the privacy of your workforce and business stakeholders. It's not a question of a trade-off between privacy and public health and safety. It's about putting the right tools and measures in place to safeguard both.

To do this, you'll need to process more personal data, e.g. collecting information about possibly infected staff and monitoring the whereabouts of teams to protect their safety and the broader business. Contact-tracing apps can help track how many people infected staff members interacted with, so you can ask them to self-isolate to prevent further spread. You could also use trackers to identify and scrub down surfaces which infected workers may have touched; equipment, photocopiers, water coolers, lift buttons, etc.

While principles such as proportionality, data minimisation, lawfulness, transparency and security continue to apply, the EU General Data Protection Regulation (GDPR) supports the use of technology under its risk-based approach to enable organisations to take on today's crisis and challenges while remaining in compliance with data protection and privacy rules.

The European Data Protection Board (EDPB) has already said that personal data will likely play an important role in the fight against the pandemic, and has confirmed that the GDPR and e-Privacy rules were designed to be flexible and can simultaneously achieve an efficient response in limiting the pandemic and protecting fundamental human rights and freedoms.

The Belgian Data Protection Authority (DPA) has received many questions from companies with regards to prevention measures being taken. While the DPA emphasised the need to respect the GDPR, it's made several declarations. Crucially, the DPA indicated that where article 9.1 of the GDPR would normally prohibit the processing of personal data concerning health, it's superseded by article 9.2 whereby it's lawful to process such sensitive data to, for example, protect the vital interests of people and/or for the public good, to the extent that organisations are doing this with sufficient measures to safeguard privacy and in compliance with the explicit guidelines issued by the authorities. In other words, processing such personal data can be acceptable.

Should an organisation put contact-tracing apps at the disposal of their workforce, in addition to the need for a lawful ground and clearly informing their people upfront, the principles of collecting only the minimum amount of data necessary and keeping it for only as long as is absolutely necessary are both to be respected (articles 5.1.c and 5.1.e of the GDPR).

In the context of preventing the further spread of the virus, an organisation or employer may not simply disclose the names of infected people, according to the principles of confidentiality (article 5.1.f) and minimum data processing (article 5.1.c). An employer may inform other employees of an infection without mentioning the identity of those involved, and the name of the infected person may be communicated to the occupational physician or the competent government services.

Use case for contact-tracing technology

Smart use of contact-tracing technology can meet the requirements embedded in the GDPR. A contact-tracing app can turn a smartphone into a beacon, once installed. The app uses a unique identifier and tracks the unique identifiers of other smartphones nearby that also have the app installed. The identity of the app user stays completely anonymous and there's no need to process geolocation data.

Once a user's been diagnosed with COVID-19, the app notifies other users that they've been in contact with an infected individual based upon the unique identifier. Organisations can consider applying a risk-based approach to trigger notification based upon the frequency and length of contact. Information storing in the app can be limited to a short period that's aligned with the incubation period and the period during which an individual's contagious, for example.

Organisations must be transparent about measures taken and adequately inform their people about processing purposes and the retention period of the personal data collected in this context (article 5.1.a), and take all necessary security measures to protect the personal data being processed (article 32).

Contact

Pascal Tops
Partner
pascal.tops@pwc.com
+32 (0)473 91 03 68

www.pwc.be/COVID-19