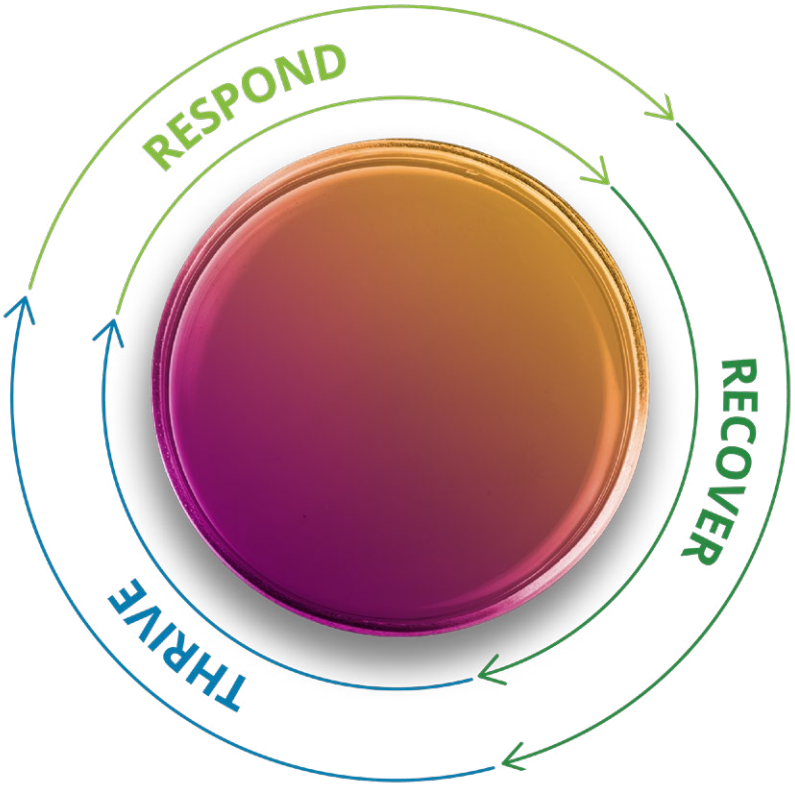
Deloitte.



Privacy and Data Protection in the age of COVID-19

By now, unfortunately COVID-19, better known as the Corona virus, has become a household name. The sudden global outbreak of COVID-19 has brought tremendous challenges to our day-to-day lives. In order to contain and mitigate the threats of this virus, governments, public and private organisations have taken several measures. These measures include among others, imposing social distancing, (where possible) mandatory teleworking, discontinuing nonessential physical meetings and promoting hand hygiene protocol.

As this health crisis evolves, many countries are hesitantly resorting to measures such as the lock-down of certain cities/countries, the suspension of flights and the closing of borders. Private organisations are creating their own plans by introducing further controls in order to comply with government measures and to protect their workforce. The overall enforcement thereof entails invasive privacy measures such as questioning individuals about their professional and private travel plans, performing temperature checks and keeping health records together with information about the possible contact with infected individuals outside the workplace.

Since these measures involve the processing of different types of personal data -including health data-, privacy and data protection is critical in their rollout. Meaning that, organisations should be aware that certain measures do have an impact on the privacy of individuals and that they have a choice where to draw the line between safety measures benefiting public health and invasive controls impacting the privacy of individuals. This last consideration should serve as a catalyst for organisations to refute the idea of the inevitable trade-off between privacy and data protection on the one hand, and effective measures protecting public health on the other. The data protection principles and the technical tools that allow striking the right balance are available to privacy professionals. Data protection is not a “yes” or “no” exercise but rather a “how to” exercise.

To address these issues and to guide governments and private organisations, numerous national Data Protection Authorities (DPAs) worldwide as well as the European Data Protection Board have published guidelines on the limits of collecting, sharing and using personal data especially relating to health in these

exceptional circumstances. In what follows, to help our clients comply with often times conflicting rules, we zoom in on a few fundamental questions and considerations that rise on the interplay between privacy and data protection on the one hand and the protection of public health on the other hand.

Does Data Protection hinder the measures that need to be taken for public health?

Within Europe, Italy was the first country to be severely impacted by the virus. Therefore, the Italian DPA (the Garante) was the first one to deliver guidelines concerning COVID-19 on the 2nd March 2020. According to the Garante, public health authorities are the only organisations that are mandated to collect and manage data about health related to the virus' spread. It states: *"The investigation into and collection of information on the symptoms typical of Coronavirus and on the recent movements of each individual are the responsibility of healthcare professionals and the civil protection system, which are the entities tasked with ensuring compliance with the public health rules that were recently adopted."* The key takeaway from the Garante was that *"employers must refrain from collecting, in advance and in a systematic and generalised manner, including through specific requests to the individual worker or unauthorized investigations, information on the presence of any signs of influenza in the worker and his or her closest contacts, or anyhow regarding areas outside the work environment."* Despite the aforementioned, employees still have the obligation to inform their employer of any danger to health and safety at the workplace.

It is important to note that after the Garante published these guidelines, the situation in Italy worsened. Therefore, the Government took very strong measures to further contain the infection, rendering the Garante's guidelines outdated. The measures included the signing of protocols between Industrial Associations and Trade Unions in order to protect workers' health. These urgency provisions allow employers to submit workers and visitors to the control of body temperature at the entrance by non-healthcare personnel, authorized by the company and without recording the data. In addition, it is also allowed to identify and record data subjects who exceed the threshold of temperature when access is prevented to company premises and a reason should be mentioned. In this case, an adequate privacy notice on the processing of personal data is required.

The Belgian Data Protection Authority (DPA) delivered its own guidelines on the 13th of March. First, the DPA mentioned that companies and employers may not rely on the vital interest of the data subject ex Article 6(1)(d) GDPR as a legal ground for processing. The current COVID-19 situation in Belgium does not justify a broad and systematic application of this paragraph. The DPA also mentioned that companies and employers may not rely on the public health processing ground ex Article 9(2)(i) GDPR with regard to processing of health data, unless they are executing explicit instructions issued by the Belgian authorities. Organisations are thus advised against "systematic and generalized" monitoring and collection of data related to health of their employees outside official requests and measures of public health authorities. Secondly, the DPA expressed that the processing of personal data collected through the measures implemented to prevent the spreading of COVID-19 must comply with all the fundamental principles of data processing of Article 5 GDPR. Thirdly, the DPA answered to frequently asked questions in relation to the processing of employee health data by employers. The publication of these guidelines was followed by the publication of resembling statements by other EEA regulators, including those of Finland, France, Czech Republic, Denmark, Germany, Hungary, Iceland, Ireland, Lithuania, Luxembourg, the Netherlands, Norway, Slovakia, Slovenia, Spain, Sweden, United Kingdom and Poland.

At EU level, Andrea Jelinek, the chair of the European Data Protection Board (EDPB) adopted a formal statement on March 16th on the processing of personal data in the context of the COVID-19 outbreak. She emphasized that data protection does not form a barrier to public health.

The EDPB updated this statement on March 19th, underlining that even in these exceptional times, the data controller and processor must ensure the protection of the personal data of the data subjects. The EDPB also stated that *"emergency is a legal condition which may legitimise restrictions of freedoms provided these restrictions are proportionate and limited to the emergency period"*. For this reason, a number of considerations are necessary to assure the lawful processing of personal data. Regarding the legal basis, employers and public health authorities do not have to rely on the individual's consent to process personal data within the scope of a pandemic but can rely on Article 6 and 9 of the GDPR. The EDPB points out that when telecom data is being processed,

such as localisation data, national laws implementing the ePrivacy Directive must also be respected. To conclude its statement, the EDPD highlights that national legal restrictions have to be considered when processing personal data in the employment context.

Finally, the European Data Protection Supervisor (EDPS) also issued a statement in response to a query from DG CONNECT of the European Commission on monitoring of the spread of the COVID-19 outbreak on March 25. The EDPS commented on 'data anonymization', stating that effectively anonymised data fall outside of the scope of data protection rules. Regarding 'data security and data access', the Commission was advised, when relying on third parties, to apply equivalent security measures and be bound by strict confidentiality obligations and prohibitions on further use as well. Finally, on 'data retention', the EDPS stressed that the data obtained from mobile operators should be deleted as soon as the current emergency comes to an end.

Does the processing of health data by public authorities open the door to surveillance?

According to the guidance from the different DPAs, private companies are not allowed to process data relating to the COVID-19 virus. However, public institutions have the possibility to rely on the legal basis from article 9 §2 i) of the GDPR. Article 9 § 2 i) allows the processing of health data when the *"processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health"*.

Despite a legal basis being at hand underpinning the processing activities of public institutions, one might not forget that the spine of data protection, more specifically, the spine of the GDPR consists of other equally important principles. Next to lawfulness, fairness and transparency, proportionality, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality need to be taken into account. However, even then there is widespread worry whether privacy and data protection will prevail in times of a health crisis.

In this context, several privacy activist groups have voiced their concerns about unprecedented levels of public surveillance. Access Now warns for the potential consequences of processing sensitive information: *"it can identify individuals and reveal highly personal details of people's lives … Collection and processing of health data, including the publication of information online, poses risks to the safety of affected persons and their communities. Health authorities should strictly adhere to a legal basis for these activities."* Privacy International, another organisation that defends and promotes the right to privacy across the world, mentions on its website that governments and international agencies are deploying extraordinary measures that might impose severe restrictions on people's rights and freedoms. Therefore, they have installed a tracker that gives an overview of all current measures that are being taken.

As the pandemic claims human lives and hospital capacities are severely tested, it calls for even more drastic measures that

further limit many fundamental human rights and freedoms, among which the right to privacy. Authorities worldwide seem to be relaxing their approach to privacy in view of the health emergency to limit contagion counting on new technologies and big data to combat the outbreak of the COVID-19 virus. Outside of the territorial scope of the GDPR, countries such as Israel are leveraging existent counterterrorism cyber technologies for COVID-19. These measures include the monitoring of citizens' mobile phone location data without their consent to track the precise movements of people infected with the virus, alert people of new cases near them and enforce quarantine measures. In fact, the Supreme Court had to intervene deciding that only those citizens who tested positive to the virus can be subject to a digital review of their movements and can receive quarantine orders from the Ministry of Health. In China, citizens are required to download government issued health applications that generate a score based on contagion risk and share that information with the police. The Chinese Ministry of Public Security has also bought a facial recognition technology that can identify individuals, even when they are wearing a (surgical) mask. In Russia, facial recognition is being used to check whether people are breaking quarantine. When looking at Taiwan, the government has integrated the national health care database with customs and travel records and is tracking whether citizens are abiding by their quarantine orders through government-issued mobile phones. Singapore implemented TraceTogether, a consent-based app to facilitate tracing efforts. South Korea has limited the spreading of contagion by extensive testing, monitoring and publicly sharing detailed information on the movements of infected citizens.

Given the effectiveness of implementing such intrusive measures and the massive impact of the virus in Europe with Italy as the epicentre, countries within the territorial scope of the GDPR are rapidly following behind. In hard-hit Italy, an anonymously monitoring solution (by using aggregated location data) was implemented, but its transparency was questioned. Many EU countries have sought collaboration with Telco's to monitor citizen movements and to push notifications to its citizens' mobile phones. In Spain the government has launched a free app to track COVID-19 cases similar to the applications developed in Asian countries. In Poland, the government has developed an app that forces COVID-19 patients to take regular selfies, to prove that they are in quarantine. The German federal government's disease prevention agency is considering using the mobile phone data of people diagnosed with COVID-19 to find potential contacts and predict the spread of the disease. Lastly, in Belgium, some technology companies are developing a health code app similar to China's health tracking application hoping to sell the solution to the government.

Conclusive Remarks

During a pandemic, it is to be expected that fundamental rights will have to be balanced against each other. The question is whether the outcome of the balancing exercise between the right to health and the right to privacy needs to be a limitation of the latter and if so, whether this limitation is necessary, proportionate and restricted in time. In any case, public authorities will need to be able to prove that they have answered those questions ex ante and not ex post. This means that even when privacy and data protection rules are being stretched several obligations cannot be abolished. Think of the fact that health data can only be processed for the purpose(s) for which it has been collected. By issuing guidance on the processing of personal data in the context of COVID-19, the DPAs emphasize the importance of the GDPR as an aspiring worldwide data protection standard. However, the current global health crisis is the first real obstacle the GDPR has to overcome since it came into force. This is an "excellent" opportunity, not only to exhibit its flexibility to harbour the needs of the public interest, but also to manifest its resilience to bounce back from temporary limitations. Privacy professionals all over the world will have to bring all their knowledge and creativity when advising on these matters.

Deloitte.