Work in Times of the Corona Virus Pandemic: Notes on the Corona Warning App

IT HAS BEEN AVAILABLE SINCE MID-JUNE: THE OFFICIAL CORONA WARNING APP. IT'S WIDESPREAD USE IS SUPPOSED TO MAKE IT POSSIBLE TO TRACK THE CHAIN OF INFECTION AND PREVENT THE SPREAD OF THE VIRUS.

Executive Summary

- In general, the employer does not have the right to order the installation and use of the app; it is entirely voluntary.
- Employees are obliged to notify the employer of any reasonable suspicion of infection.
- Employers must comply with data protection laws.

If an encounter of sufficient duration and of short distance occurs between app users, the app exchanges randomly generated ID codes via the Bluetooth interface of the users' devices and stores them on the respective smartphones. If a user reports an infection, the affected IDs are sent to a central server. The app retrieves them from the server and compares them to the IDs on the user's own device collected from past contacts. If contact with an affected ID is detected in this way, the individual risk of infection is determined based on the duration and distance profile. The user is informed about the contact and receives recommendations for action. Data is not automatically passed on to third parties, such as the employer or health authorities.

The benefits and effects of the app, the costs associated with its development and operation, data protection and voluntary vs. mandatory use are the subject of lively discussion.

What should employers and employees do from an employment law perspective with regard to the Corona Warning App?

Can employers demand use of the app?

The app is meant to be used on a voluntary basis. There is (at this time) no legal basis for a government order that could make its use mandatory.

But do employees have this choice vis à vis their employer?

Can employers order employees to use the app in order to reduce the risk of infection among their staff and thus fulfil their duty of care?

The admissibility of such a far-reaching order is closely linked to a careful weighing of the interests worth protecting in each case: Do the employee's personal rights and the protection of his or her privacy outweigh the employer's interest to protect the company?
The following principle applies:
The higher the employer's interest in the information and the less severe this impacts the employee

personally, the more likely it is that an authority to order the use can be justified.

The app works anonymously; no further data is collected or stored apart from the information whether there has been sufficient contact with another person. The employer has no access to data generated with the app.
From the employer's point of view, the app can increase safety in the company because potentially infected individuals are warned before symptoms occur. **Particularly in the case of business activities with frequent customer contact or external work, the app can quickly detect potentially dangerous contacts.**

However, to assess a contact the app cannot take into account protective measures such as masks or glass panes, so the risk assessment is not always adequate. In addition, the app can only reliably determine a risk if, on the one hand, the respective contact persons also use the app and if, on the other hand, the employee constantly has the smartphone with the activated app on him/her.

An employer's order to install and use the app on the employee's private smartphone is likely to be inadmissible because it would constitute usage of the employee's private property and would also affect the employee's private life. It would be an equally inadmissible encroachment on the employees' privacy to demand that they keep a business phone on them at all times. Considering the overall gain of information is rather limited, it is unlikely that such an order affecting the conduct of a person's private life would be deemed permissible when weighing the respective interests.
Even if the employer interests outweighed the employee's interests in the individual case and an order – concerning only the business phone – would be admissible, the actual use of the app still depends solely on the employee's participation; the employer has no means of exercising any kind of control.

Considering the legal and factual difficulties, it is therefore not advisable to issue an order to use the app. It can probably best fulfil its certainly useful support function if the decision about its use is left to the individual user.

Obligation to notify the employer

What happens if the employee does use the app and it detects a risk of infection? The app itself does not initiate any measures; that is entirely up to the user.

In principle, employees do not have to report a suspected illness to their employer, nor do they have to inform the employer of the nature of an illness. However, this does not apply if there is a situation in which the employer must take measures to protect other employees or other persons possibly affected, such as customers.

In view of the increased risk of infection and the resulting duty of protection on the part of the employer, the employee is therefore obliged to provide information in the case of highly infectious diseases such as COVID-19.

If the employee is aware – through the use of the app or in any other way – of a suspected infection or increased risk affecting him/her, the employer must be notified.

This obligation results from the mutual duties of considerateness and support that exist in the employment relationship: employers can only comply with their duty of protection and take necessary protective measures for others, if the employee notifies

them. Should an employee not comply with this obligation this can be sanctioned under employment law.

Data protection

When handling relevant employee information, confidentiality and data protection regulations must of course be observed – information can only be passed on to the extend of what is absolutely necessary.

Measures in case of a suspected infection

If an official quarantine order or a prohibition to work is issued due to a suspected infection, the employee will not be able to continue working. For up to six weeks, the employee is entitled to payments compensating the amount of the lost salary in accordance with the Infection Protection Act, for which the employer will be reimbursed by the authorities upon application.

If there is an increased risk of infection, the app recommends avoiding all contact. If, however, no official measures are taken, employer and employee must agree on the further procedure in the individual case. The employer faces legal duties of care and protection with regard to the safety and health protection of all employees, the affected individual and colleagues. This also includes the best possible prevention of infection risks at the workplace. Therefore, the employer will also have to take action in case of an increased risk – determined by the app or otherwise. Depending on the situation, operational circumstances and the person concerned, various measures may be taken into consideration, such as the allocation of an individual office, home office arrangements or even temporary leave from work with continued pay.

Our recommendations

As part of the corona virus crisis management, employers should inform their employees (among other things) about the Corona Warning App. Employers may make a recommendation for installing the app, but the decision on whether to use it or not should be made by the employee. Employers can inform staff about whether installing the app on the employees' business phones is allowed in case an employee wishes to do so. Employees should be made aware of existing notification obligations in the event of a corona virus infection, but also in relation to a suspected infection or an increased risk. The employer should appoint contact persons for this purpose and ensure that everyone involved is aware of and complies with the principles of confidentiality and data protection regulations applicable in this context.

Wolfgang Boehm
Lawyer
Specialist lawyer for employment law
Heidelberg
wolfgang.boehm@gsk.de

Nicole Deparade
Lawyer
Heidelberg
nicole.deparade@gsk.de

GSK
STOCKMANN

Copyright
GSK Stockmann – all rights reserved. The reproduction, duplication, circulation and/or the adaption of the content and the illustrations of this document as well as any other use is only permitted with the prior written consent of GSK Stockmann.

Disclaimer
This client briefing exclusively contains general information which is not suitable to be used in the specific circumstances of a certain situation. It is not the purpose of the client briefing to serve as the basis of a commercial or other decision of whatever nature. The client briefing does not qualify as advice or a binding offer to provide advice or information and it is not suitable as a substitute for personal advice. Any decision taken on the basis of the content of this client briefing or of parts thereof is at the exclusive risk of the user.

GSK Stockmann as well as the partners and employees mentioned in this client briefing do not give any guarantee nor do GSK Stockmann or any of its partners or employees assume any liability for whatever reason regarding the content of this client briefing. For that reason we recommend you to request personal advice.

www.gsk.de

GSK Stockmann

BERLIN
Mohrenstrasse 42
10117 Berlin
T +49 30 203907-0
F +49 30 203907-44
berlin@gsk.de

HEIDELBERG
Mittermaierstrasse 31
69115 Heidelberg
T +49 6221 4566-0
F +49 6221 4566-44
heidelberg@gsk.de

FRANKFURT / M.
Taunusanlage 21
60325 Frankfurt am Main
T +49 69 710003-0
F +49 69 710003-144
frankfurt@gsk.de

MUNICH
Karl-Scharnagl-Ring 8
80539 Munich
T +49 89 288174-0
F +49 89 288174-44
muenchen@gsk.de

HAMBURG
Neuer Wall 69
20354 Hamburg
T +49 40 369703-0
F +49 40 369703-44
hamburg@gsk.de

LUXEMBOURG
GSK Stockmann SA
44, Avenue John F. Kennedy
L-1855 Luxembourg
T +352 271802-00
F +352 271802-11
luxembourg@gsk-lux.com