THOMSON REUTERS

REGULATORY INTELLIGENCE

To test, or not to test? Key data protection considerations for reopening workplaces in the EU

Published 29-May-2020 by
Bridget Treacy and David Dumont, Hunton Andrews Kurth

As COVID-19 infection rates level out and decline across Europe, businesses are now turning their attention to re-opening their workplaces. Unlike the lockdown process, which in many countries was swift and sudden, there is more time to plan the re-opening of workplaces, and to consider how best to reassure staff and provide a safe environment for them and for visitors. In addition to health and safety, and employment law requirements, there are several important data protection considerations that arise. Perhaps the most often asked question at this point is whether employers can (or should) test their staff for COVID-19.

Does EU data protection law permit testing in the workplace?

There are three types of tests that employers might consider: temperature checks; antigen tests; and antibody tests. Most businesses are currently considering temperature checks. Whether conducted using thermal scans, infrared thermometers or disposable thermometers, these checks potentially involve the capture of health data, which is considered 'special category' personal data under the European General Data Protection Regulation (2016/679) (GDPR) and accordingly is subject to additional safeguards. The European Data Protection Board (the EDPB) issued a statement on March 19, 2020, confirming that in the context of COVID-19, organisations should generally be able to invoke their legal obligations to ensure employees' health and safety, reasons of public interest, and/or to ensure employees' or other individuals' vital interests, as a legal basis for processing employees' health-related data.

In addition to satisfying a legal basis for processing, other legal requirements for processing personal data will also need to be met in the usual way. In brief, employers will need to avoid any unnecessary collection of personal data, avoid retaining it for any longer than necessary and ensure that processing is legitimate, proportionate and limited to what is necessary to achieve the stated objective. Temperature checking may be considered proportionate in large, open-plan offices or factories with hundreds of employees. In smaller offices, where employees are able to socially distance and do not share communal areas, temperature checks may be considered disproportionate to the risks presented.

Employers will also need to consider how to inform staff that their data will be processed. If a temperature check can be conducted without collecting personal data, any notice should inform employees that the checks do not involve processing of their personal data. Notice should be provided before the temperature check is carried out and could, for example, be posted at the entrance to an office or emailed to employees before they return to work. After receiving this notice, the employee should have the opportunity to refuse the check.

Permissive EU jurisdictions for temperature testing

The regulatory approach to conducting temperature checks differs across the EU. The UK is among the more permissive jurisdictions, with the Information Commissioner's Office emphasising the importance of ensuring lawfulness, fairness and transparency in the collection and processing of employee health data. In the COVID-19 context, employers in the UK are permitted to carry out temperature checks on employees, assuming that appropriate safeguards are in place and that the measures are considered to be necessary to protect the workforce.

Similarly, the Irish data protection authority has not ruled out temperature checks, but stated that more intrusive requirements, such as requiring employees to complete health questionnaires, would require "strong justification based on necessity and proportionality and on an assessment of risk". In Spain, temperature checks are permitted provided that they are based on criteria defined by the competent health authorities, that individuals have an opportunity to respond to any decision to refuse them access to premises if their temperature is higher than normal, and provided that temperature data is not recorded or retained. In Italy, temperature checks are permitted provided that the process for collection complies with data protection and employment law requirements.

Restrictive EU jurisdictions for temperature testing

Other EU data protection regulators have taken a more restrictive approach to temperature testing. In the Netherlands, France, Luxembourg and Hungary, data protection regulators have sought to ban temperature checks by employers altogether. The French and Dutch regulators have conceded, however, that the checking of temperatures alone (where the result is not recorded in any way and not processed using automated means), would not technically constitute processing under the GDPR, and as such would likely fall outside its scope. In addition, in some jurisdictions, such as Hungary, it is possible for the employer to require that a health check be carried out by a health professional and that the results are provided to the employer, but only where this is absolutely necessary for

the specific position of the employee. Other regulators, such as in the Netherlands, have also specified that health checks may only be conducted by a company doctor.

Interestingly, several regulators (including the German and the Austrian data protection regulators) have noted that since temperature is not an entirely reliable symptom of COVID-19, the usefulness of temperature checks in an effort to prevent the spread of COVID-19 is questionable.

Further, a number of EU data protection regulators (such as the Swedish and Dutch) defer to employment law requirements, for example, in considering whether an employee exhibiting symptoms or reporting a high temperature can be required to go home. Employment law considerations are important in this context, and specific legal advice should be sought in key jurisdictions.

Practical safeguards

Turning to consider how temperature checks could be implemented, many businesses have sought to adopt a conservative approach. While specific advice should be sought in key jurisdictions, examples of typical steps might include the following:

Provide the opportunity for employees to check their own temperature.
Encourage employees to self-report symptoms of COVID-19 privately and, if possible, create dedicated channels through which they can do so.
Request information relating to possible exposure to the virus in the first instance (e.g. Has the person travelled recently? Have they used public transport to commute to the workplace? Have they had known interaction with someone exhibiting COVID-19 symptoms?)
If answers to these preliminary questions raise flags, it may then be proportionate to take further steps such as referring the employee to the company doctor for a temperature check or requesting that the employee works from home as a precaution.
Require a company doctor to perform and record any health checks.

Accountability

Finally, it should be noted that in the EU, all businesses must be able to demonstrate how they comply with their data protection obligations. A key accountability measure is a data protection impact assessment (DPIA), which should be carried out prior to the commencement of the processing activity in question (temperature checks in this instance) in order to identify the risks posed to employees.

Employers should also ensure that those conducting the checks are appropriately trained and aware of their data protection obligations. In addition, employers should ensure that they have internal documentation in place recording how this processing complies with the data protection principles, including practices regarding storage and retention or deletion of the data.

Complaints Procedure

Produced by Thomson Reuters Accelus Regulatory Intelligence 01-Jun-2020

About the authors

Bridget Treacy *is a partner in the firm's global technology, outsourcing & privacy group in the firm's London office and leads the UK Privacy and Cyersecurity team. Her practice focuses on all aspects of privacy, data protection, information governance and e-commerce issues for multinational companies across a broad range of industry sectors. Bridget's background in complex technology transactions (including wide-ranging experience of advising on sourcing agreements, strategic alliances and other collaborative arrangements with a technology focus) enable her to advise on the specific data protection and information governance issues that occur in a commercial context. She can be reached at +44 (0)20 7220-5731 or btreacy@HuntonAK.com.*

David Dumont *is a partner in the firm's global technology, outsourcing & privacy group in the firm's Brussels office. David assists large, multinational clients with various aspects of EU privacy and data protection law. As a result of his extensive experience in this area, he has developed a strong knowledge of the key privacy and data protection issues companies are facing. He can be reached at +32 (0)2 643-58-18 or ddumont@HuntonAK.com.*