LK SHIELDS
YOUR LEGAL COUNSEL

INTELLECTUAL PROPERTY

Coronavirus and Business Interruption: Data Privacy and Compliance Challenges

by

Coronavirus and Business Interruption: Data Privacy and Compliance Challenges

9th March 2020 | by

As you keep your staff safe during an emergency, take care to ensure that regulatory aspects of your reaction are considered.

The global coronavirus crisis has taught us that an ongoing public health emergency needs to be added to a list of business threats – besides flooding and volcanic ash cloud. Here are three tips for implementing your contingency plans in a manner which reduces compliance risk.

Staff safety – a privacy problem?

Employers are considering a wide range of options to reduce the risk of infection at the workplace. Homeworking and flexible working arrangements can be an effective way to mitigate the risk of staff exposure and presumably you have the appropriate employment and data protection policies and procedures, which permit and govern these types of working arrangements, already in place.

During an emergency, an employer typically enjoys a wide margin of discretion when reorganising its daily operations. In the case of Covid-19, a company might roll out mandatory staff training or require the use of disinfectants. However, the question of probing into the personal circumstances of your staff is more complicated. Can you ask Bob in Finance about his recent family holiday, for the sake of the health and safety of your broader workforce?

What appears to begin with an innocuous question may have considerable ramifications for the employee, if subsequently asked to stay at home, or for you, if the spotlight turns onto your personnel procedures and records.

In essence, conversations with staff about their private lives may constitute a form of monitoring and possibly profiling. A narrow margin of discretion applies to employers in relation to both activities at the workplace and you need to be able to justify your approach.

An employer's reliance on employees' consent as a legal basis to process their personal data is problematic. This is because of the perceived unequal power dynamic between an employer and its employees. You need to establish if there is another reason in law to have such discussions and how to appropriately conduct them, as well as taking into account your existing company policies and applying them in a non-discriminatory way.

Just checking the temperature?

You may also be prompted by your staff to investigate a colleague's flu-like symptoms. This leads you to consider the question of whether you can test his or her temperature at the workplace and/or send him or her to the company's physician.

At issue here is the fitness to work of the employee and your obligation to protect the workforce, for example, for health and safety or public interest in the area of public health (at the time of writing, no

Governmental order has issued on this net issue). You need to ascertain if, why, and how you will implement mandatory legal testing in practice. Again, broader considerations of employment equality, data protection, and privacy laws apply and must be considered. Also, the existence of a crisis does not justify departure from established company policies and best practice.

You should carefully identify the precise lawful basis for your testing and review how you provide sufficient information to your staff on this issue. What will you test, when will you test, who will be tested, who carries out the tests and on the basis of which service contract, what happens with the results, how long will they be retained and what are the consequences?

Existing employee privacy policies and procedures should be reviewed and enhanced, where necessary, to ensure they address any future obligation to conduct health examinations of employees in the case of public health emergencies or generally. Given that health data is highly regulated and these tests are generally considered as intrusive, proceeding with caution is necessary.

Third party disclosure?

In a crisis, you may need to liaise with relevant authorities to ensure the safety of your staff. In the case of Covid-19, for example, you may work with the HSE and/or other state authorities in order to facilitate contact tracing and other public health measures.

However, even in a crisis, you are required to follow compliant procedures. There are a number of preparatory steps you should consider before making any disclosure of staff personal data. For example, satisfy yourself as to the nature and scope of the request, identify only relevant personal data, establish your legal grounds for disclosure, ensure that this legal basis is communicated to staff and ensure any disclosure of personal data is performed in a secure manner. Ensure that your DPO, if applicable, is closely involved in such decisions and that employee privacy is protected in line with laws.

Your duty of care to your workforce includes your duty to treat their personal data, and in particular their medical data, in accordance with your data protection obligations. In a crisis, if in doubt, seek advice prior to any disclosures, and take care that internal communication of such data is limited to those who strictly need to know it.

For more information, please contact Aideen Burke at aburke@lkshields.ie. To read our Coronavirus guide for employers, please click here.

About the Author