



CORPORATE AND COMMERCIAL

Following the Protocol? Don't Forget Staff's Data

by **Jane O'Grady**

Following the Protocol? Don't Forget Staff's Data

13th July 2020 | by Jane O'Grady

While planning your return to workplace strategy, ask yourself: do your current data protection policies and processes cover your new COVID-19 prevention and control measures?

On 9 May 2020, the 'Return to Work Safely Protocol' (Protocol) was published by the Department of Business, Enterprise and Innovation (DBEI) and the Department of Health to provide a framework of measures that employers and workers must follow to manage and reduce the spread of COVID-19 in the workplace.

Many of these measures require the processing of workers' personal data in ways that were not foreseen by employers in 'pre-COVID times'. Employers must now review and update their workplace data protection policies and procedures to reflect their plans to implement the Protocol. Helpfully, the DBEI and the Data Protection Commission (DPC) have recently published separate guidance that will assist employers in complying with Irish data protection laws when doing so.

DBEI Guidance on the Protocol

The Protocol provides a non-exhaustive set of measures, several of which necessarily involve the processing of workers' personal data, including special categories of personal data (e.g. health data). We have commented below on measures that have been specifically identified in the DBEI's recent guidance.

(a) Return to work form

Employers must provide their staff with a form to be completed and returned to the employer before they can re-enter the workplace. Its purpose is to ensure that workers are aware of the symptoms of COVID-19 and allow employers to make informed decisions about a worker's return.

The Protocol specifies five questions that must be included in the form, all of which concern COVID-19 symptoms. Also, the Protocol requires workers to inform their employer of any other personal circumstances, not covered by the five questions, that may need to be disclosed to allow their safe return (additional information).

The DPC's guidance highlights that these forms should be tailored to observe the data protection principle of data minimisation. Instinctively, a controller may determine, on this basis, that their form should only allow workers to provide 'Yes/No' answers to the questions prescribed by the Protocol, and that the form should not contain any text box facilitating the provision of additional, and possibly irrelevant, information. However, the DBEI's guidance indicates that the form may include a sixth question, asking workers to disclose any additional information.

If employers include a text box allowing workers to provide additional information on the return to work form, they should consider including clear instructions that only COVID-19 related information should be disclosed.

The DBEI's guidance informs employers that the form should not be retained once a worker has returned to

the workplace. This means employers must delete or shred the form once the staff member is back in the workplace, or return the form to them at that time.

(b) Contact tracing logs

Employers must keep a log of workers who are in close contact for extended periods during their working day (e.g. working together in spaces where social distancing guidelines may be difficult to maintain).

The DBEI's guidance highlights that these logs should contain the minimum amount of data necessary to facilitate the Health Service Executive's (HSE) official contact tracing procedures and to assist workers as a memory aid when reporting their close contacts to the HSE. The log should not be used for any other purpose, and its retention should be in line with HSE guidelines. The DPC's recent guidance provides that when maintaining this log, employers must ensure they do not disclose a particular worker's COVID-19 diagnosis to other workers.

(c) Workers' individual risk factors

Employers will need to consider what special accommodations must be put in place for workers who are at higher risk from the virus (e.g. older persons and those with underlying medical conditions) or who are living with persons who are at higher risk. This will necessitate processing workers' personal data (e.g. a person's age) for new purposes, which would not have been done prior to the outbreak of the virus. Also, employers are likely to receive health-related data of its workers and their household, which would not have been required before the pandemic.

The DBEI's guidance expects employers to ensure workers know how to inform their managers of these risk factors in a confidential manner. The DBEI also highlights employers' obligation to maintain the confidentiality of health data and recommends appointing a designated person to oversee this process for this purpose.

Employers should already be aware of their duty of confidence and also their ongoing GDPR obligations to keep personal data confidential and secure. Employers should bear in mind that the Data Protection Act 2018 (DPA) obliges them to implement 'suitable and specific measures' (Section 36 DPA) when relying on certain legal grounds that may be available to them when processing workers' health-related data. Such safeguards may include limiting access to personal data, strict time limits for erasure and targeted staff training.

Other Measures Required by the Protocol

The Protocol includes a number of requirements, in addition to those highlighted above, that will necessitate the processing of workers' personal data. These include:

(a) Workers must report to their manager if any COVID-19 symptoms develop during their working day. In these circumstances, the employer must follow certain steps including carrying out an assessment of the incident and providing advice and assistance to the HSE, if requested. This will require employers to implement measures for the receipt and response to such notification (e.g. privacy focussed training, activation of a pre-formulated response plan and documenting incidents).

(b) Employers must provide for physical distancing across all work activities. The Protocol envisages employers adapting existing sign-in and sign-out measures at the workplace to ensure that physical distancing can be maintained. The introduction of any new sign-in or access control measures will likely involve data protection and privacy considerations. Whilst the Protocol refers to the use of biometrics in the workplace, maintaining such measures 'post-COVID' may be problematic under Irish data protection law. This should be considered before investing in such technologies.

(c) Workers must receive induction training on their return to the workplace and employers must consult with them and provide ongoing communications relating to workplace prevention and control measures and advice issued by Irish public health bodies.

Employers will need to include these processing activities in updated workplace privacy notices and

incorporate them into their overall data protection compliance framework.

Temperature Testing

The Protocol anticipates an obligation on Irish employers to 'implement temperature testing in line with public health advice'. However, there is currently no public health advice that requires Irish employers to submit employees (outside of healthcare and residential care settings) to mandatory temperature testing. The DPC's guidance highlights that in the absence of public health advice recommending workplace temperature testing, such measures should not be considered as required under the Protocol.

Irish data protection law does not preclude an employer from conducting temperature testing of employees. However, an employer intending to do so must carefully consider current public health advice, employment law and data protection law. In this regard, the DPC's guidance indicates its expectation that such testing should only be introduced as a COVID-19 response measure in the context of 'a particularly high-risk workplace and in response to a particular risk that has been identified' and this should be justified pursuant to a documented data protection impact assessment (DPIA).

Legal Grounds

These new processing activities must be based upon appropriate legal grounds provided under Article 6(1) and Article 9(2) GDPR. The processing of COVID-19 symptoms and additional information provided by workers must be based on appropriate grounds under Article 9(2) GDPR and relevant sections of the DPA.

The DPC's guidance highlights the well-established position that an employee's consent (Articles 6(1)(a) and 9(2)(a) GDPR) is unlikely to be an appropriate legal basis to process their personal data. Employees are almost never in a position to freely give, refuse or revoke consent, due to the nature of the employer and employee relationship.

Article 9(2)(b) GDPR may be an appropriate legal basis to process workers health data, where this is necessary to carry out legal obligations imposed on employers, for example ensuring the health and safety of individuals in the workplace under the Safety, Health and Welfare at Work Act 2005. Section 46 DPA requires employers to take 'suitable and specific measures' (as set out in Section 36 DPA) when relying on this legal basis.

Article 9(2)(i) GDPR may be relied upon to process workers' health data where this is necessary, for example, to follow guidance or directions issued by public health authorities or other relevant authorities. This legal basis must be read together with Section 53 DPA, which requires employers to take 'suitable and specific measures'.

Other GDPR legal grounds will be relevant when implementing the Protocol. Employers should consider all GDPR legal grounds and any relevant sections of the DPA in light of their planned COVID-19 prevention and control measures. These legal grounds must be communicated to employees in an Article 13 GDPR compliant privacy notice.

Workplace Privacy Notice

A key data protection step that must be addressed before workplaces are reopened will be to provide workers with the return to work form and a privacy notice detailing the new processing activities consequent to these new measures. Many employers are choosing to provide their workers with these documents as part of a single pre-return communication.

Employers may amend their existing workplace privacy notices to reflect their new processing activities. Alternatively, they may supplement their existing privacy notices with a notice that only deals with the new ways in which workers' personal data will be processed in response to the virus. This approach may enable employers to provide their workers a relatively short form notice, which can be subsequently modified to reflect any new public health advices or revised COVID-19 response measures, thereby minimising changes to existing 'pre-COVID' notices.

As public health advice continues to evolve, the ways in which organisations may need to process workers'

personal data may change. Employers will need to ensure they inform workers of these changes and update workplace notices, policies and procedures accordingly.

The cross-disciplinary business crisis advisory team at LK Shields are available to provide practical advice and legal insights to employers, business owners, directors, insurance providers, compliance officers, HR professionals and decision-makers faced with a crisis.

If you would like to discuss this further, please contact crisis-advisory@lkshields.ie or any member of our business crisis advisory team. To subscribe to our crisis advisory news and insight please [click here](#).

About the Authors



Jane O'Grady
Partner

Jane is dual qualified as a solicitor and a trade mark and design attorney, with many years' experience advising on commercial contracts, intellectual property, commercial agency and all aspects of technology law.

T: +353 1 637 1554 **E:** jogrady@lkshields.ie