

Vaccination status and office re-openings: a match made in heaven or a cloud to a silver lining?

Aoife Mac Ardle, Associate, and Lisa Leonard, Associate, at McCann FitzGerald explain the data protection issues for employers seeking vaccine information status from their employees

As 2021 has unfolded, we've seen the rollout of Covid-19 vaccines and the reopening of many sectors of the economy. For office workers, who have largely been working from home since the onset of the pandemic, the potential reopening of their workplaces has come into view. Employers preparing to open the office doors again will be looking to see how this can be facilitated safely and in line with public health guidance.

Increasingly, employers keen to ensure reopening or greater use of workplaces are considering seeking details of vaccination status in connection with workplace safety measures. The use of vaccine status as a safety measure has, however, generated concerns about data protection, employee privacy and freedom to make health choices.

In this article, we consider the data protection issues arising in connection with an employer seeking vaccination status information from employees. We look at recent guidance, the underlying legislation and recent development to see how employers should be weighing data protection considerations in this area.

What is the official line on using employee vaccination status for safety purposes?

The Government's "Work Safely Protocol: COVID-19 National Protocol for Employers and Workers" (May 2021) discusses the rollout of Covid-19 vaccines in Ireland. However, it notes that the vaccine programme is optional and that irrespective of the roll-out, public health infection prevention and control measures (including social distancing, masks and adequate ventilation) all need to remain in place. As such, the Government's current position (which was last updated in May) is that seeking details of the vaccination status of employees generally is not, as of the time of writing, a necessary measure to ensure a safe workplace.

More recently, the Data Protection Commission (the 'DPC') published guidance on processing Covid-19

vaccination data in the context of employment (June 2021).

The DPC expressed its view that there was a lack of a clear legal basis for an employer to process such personal data. The DPC questioned the necessity for this information in the employment context and pointed to the voluntary nature of the vaccination programme itself. In this respect, the DPC drew a link between its guidance and the Work Safety Protocol, as the DPC noted that the Protocol did not foresee establishing vaccination status as a necessary safety measure except in limited circumstances. The DPC guidance did, however, note that vaccination status data could be considered a necessary safety measure based on sector guidance, specifically noting the Medical Council's Guide to Professional Conduct in this respect.

While the DPC's guidance has cast doubt on an employer's ability to seek details of vaccination status from employees except in limited circumstances in compliance with data protection law, it is noteworthy that the DPC's position on the apparent absence of a legal basis for this processing is expressly linked to current government public health advice on safety measures. As the past year has shown, government public health advice may change in response to the nature of the threat from the virus (which is acknowledged in the DPC's guidance). In addition, it is interesting that the DPC's guidance contemplates a sector by sector assessment of what is necessary to ensure safety at work. This aspect of the guidance indicates that the purpose for which an employer is seeking to process vaccination status data is critical for determining whether the employer has a legal basis for such processing.

What are the underlying data protection issues for employers considering proof of vaccination as a safety measure?

From a data protection perspective, in addition to an employer's general obligations in respect of employee

data processing (e.g. transparency requirements), there are four key areas for consideration when designing a return to office plan that might entail seeking vaccination status data from employees:

- Purpose of processing;
- Data minimisation and Article 5(1)(c) GDPR;
- Legal basis for processing and Article 6 GDPR; and
- Health data and Article 9 GDPR.

Purpose of processing

As mentioned above, the purpose for which vaccination status data will be processed by an employer is central to any data protection analysis of this issue. Is it intended that vaccination status will be used to determine who may or may not attend the workplace, what public health measures (such as social distancing) ought to be maintained, etc? The Work Safely Protocol, which currently states that public health measures ought to be maintained regardless of the vaccination rollout, will be an important consideration in this context.

Data minimisation and Article 5(1)(c) GDPR

Article 5(1)(c) GDPR provides that processing must be limited to what is adequate, relevant and necessary for the purpose of processing. The key question for an employer considering seeking vaccination status from their employees to consider is whether this information would be necessary in connection with the purpose(s) for which the data will be used or are there other (less data intrusive) means of accomplishing this.

In circumstances where many employees have been working from home for lengthy periods, and where those who could not work from home have been relying on public health measures such as physical distancing, mask wearing and ventilation as safety measures (as recommended

“The key question for an employer considering seeking vaccination status from their employees to consider is whether this information would be necessary in connection with the purpose(s) for which the data will be used or are there other (less data intrusive) means of accomplishing this”

in the Work Safely Protocol), a question to be addressed by any employer considering seeking details of vaccination status is why are they seeking it now? Does the employer have good reasons for wishing to have more employees attend their workplace in safety that would be facilitated by obtaining vaccination status details? It may be the case that public health measures such as social distancing, mask wearing, ventilation etc. cannot be

relied on by themselves to maintain safe working environments and that obtaining vaccination status data would be an additional tool to be implemented for these purposes. Whatever the rationale might be, the onus will be on an employer to be able to identify why it is necessary to seek vaccination status details.

Legal basis for processing and Article 6 GDPR

For any processing of personal data, Article 6(1) GDPR states that the processing is lawful only where one of the conditions listed in subsections (a) to (f) apply. For the purpose of seeking details of vaccination status in an employment context, the legal bases most likely to be relevant are that this is necessary for the purposes of legitimate interests pursued by the employer or consent.

Taking these in turn, Article 6(1)(f) –

necessary for the purposes of legitimate interests pursued by the employer or a third party - would appear to be the most relevant legal basis. An employer is likely to have legitimate interests in connection with reopening or increasing the use of their ‘ordinary’ place of work and doing so in a way that is safe for people attending its premises. A key part of the analysis is for the employer to consider carefully their specific interest in physical attendance of employees. Until the pandemic ends, a general interest in full time attendance for all employees is unlikely to be sufficient as a legitimate interest.

The difficulty for employers, in common with the other legal bases, is that the processing must be necessary for the legitimate interests being pursued, so the interests must be specific and tailored. The challenge for employers considering relying on legitimate interests is that these must be balanced against the interests and fundamental rights and freedoms of the affected data subjects. It is likely that the interests being pursued will need to be substantial to ensure that they would not be overridden by employees’ rights and freedoms in this context.

A potential alternative legal basis would be to seek consent of the employees, which overlaps with a relevant exemption under Article 9 GDPR discussed below. Consent under the GDPR needs to be freely given, which crucially requires a real ability for the employee to refuse to provide their consent.

Typically, consent is not relied upon in the employment context as the imbalance of power in the employment relationship makes it difficult to meet the standard required. This is specifically noted by the DPC in its guidance on vaccination status.

In order to meet this high threshold, where an employer is considering relying on consent as its legal basis for seeking vaccination status information, there would need to be a real alternative system in place to counteract this imbalance of power, so that employees who decline to provide the information are not effectively excluded or isolated from other staff

(Continued on page 8)

[\(Continued from page 7\)](#)

members. Even if there was, reliance on consent might be vulnerable to challenge on the basis that it could not properly be regarded as having been freely given.

Health data and Article 9 GDPR

Article 9(1) GDPR provides that data concerning health should not generally be processed unless one of the exemptions contained in Article 9(2) GDPR applies.

An individual's vaccination status in respect of a particular disease would constitute health data, so employers would need to be able to identify an exemption under Article 9(2) to process it. At the present time, the exemptions most likely to be relevant for employers are explicit consent (Article 9(2)(a)), necessity for employment obligations (Article 9(2)(b)) and necessity for assessment of working capacity of an employee (Article 9(2)(h)). If the public health situation were to become grave, necessity for reasons of public interest in the area of public health (Article 9(2)(i)) or necessity for reasons of substantial public interest (Article 9(2)(g)) could also come into play.

With respect to the explicit consent exemption, Article 9(2)(a) requires that the consent is explicit, which implies a higher standard of consent than that required under Article 6(1). Again, the existence of a real alternative to providing vaccination status to the employer will be important to the validity of any consent under the GDPR. The employee must have a genuine ability to say no to the processing operation. Where employees feel pressured into saying yes due to a lack of alternative options, the consent will not meet the standard required.

With respect to Article 9(2)(b), this exemption concerns obligations of the employer in the field of employment law. As regards vaccination status data, there is an argument that the employer's duties under the Safety, Health and Welfare at Work Act 2005 may require the collection of this information to ensure a safe place of work.

The potential weakness in relying on this exemption is that collection of vaccination status data is not a specific requirement of employment law (as yet). Instead, the employer would be relying on its requirement to conduct a safety assessment, which is legally required, as its basis for seeking vaccination status data, if the collection of such data was properly considered to be necessary for the purpose of the safety assessment. Different views could be taken on whether this would be sufficient to meet the requirements of Article 9(2)(b), in light of the sensitive nature of the data processed.

With respect to Article 9(2)(h), this exemption relates to assessment of the working capacity of an employee, which in this case is whether they can safely attend the office. As outlined above in the discussion about 'necessity' and data minimisation, it will be important for an employer to consider the capacity of the employee vis-à-vis their work and whether they are carrying out work that must necessarily be performed in the office environment. Where the work could be performed from home, it may not be possible to rely on this exemption, as vaccination status would not be relevant to consider the working capacity of an employee who could work from home.

Could the Digital COVID Certificate be used to ensure a safe office work environment?

Since the EU Digital COVID Certificate is being used in connection with facilitating the reopening of indoor dining, questions have arisen as to whether it could also be used in connection with reopening of office work environments. It seems unlikely, however, that this could arise without substantial new legislation facilitating it.

This Digital COVID Certificate was formally introduced by Regulation (EU) 2021/953 (the 'Regulation') and has been operating in Ireland with respect to travel since 19 July 2021. Under the Health (Amendment No. 2) Act 2021 (the 'Health Amendment Act'), the Irish legislature has enabled

it to be used as evidence of vaccination or recovery from Covid-19 for the purposes of determining who may be permitted to access indoor service in bars and restaurants since 26 July 2021.

What is the Digital COVID Certificate?

The Digital COVID Certificate consists of three possible certificates:

- Vaccination certificates;
- Test certificates; and
- Recovery certificates (demonstrating recovery from Covid-19 within the previous 180 days).

In line with the principle of data minimisation, the Digital COVID Certificate only contains personal data strictly necessary for the purpose of facilitating the exercise of the right to free movement, and the specific data fields are set out in the Regulation.

What is the legal framework around it?

Article 10(2) sets out the limited scope for the Digital COVID Certificate, stating its use shall only be to "facilitate the exercise of the right of free movement within the Union during the COVID-19 pandemic", which is also stated in the Regulation's recitals.

These recitals note that Member States may process the personal data contained in the Digital COVID Certificate for other purposes, provided that the legal basis for the processing of such data for other purposes is provided for in national law. Any such national law must comply with data protection law, and the principles of effectiveness, necessity and proportionality, and "should contain provisions clearly identifying the scope and extent of the processing, the specific purpose involved, the categories of entity that can verify the certificate as well as the relevant safeguards to prevent discrimination and abuse, taking into account the risks to the rights and freedoms of data subject".

Article 10(2) further states that where the certificate is used for non-medical purposes, personal data accessed during the verification process should not be retained.

What are the concerns?

These provisions, which tie the use of the certificate to free movement and any further use to the passing of legislation by Member States, reflect comments from the European Data Protection Board ('EDPB') and European Data Protection Supervisor ('EDPS') in a joint opinion on the proposal for the Digital COVID Certificate issued on 31 March 2021 (the 'Opinion').

The Opinion expressed concerns about the use of the certificate outside the context of free movement, stating that such further use may lead to unintended consequences and risks to the fundamental rights of EU citizens.

The Opinion also noted that any further use of personal data contained in the Digital COVID Certificate must respect Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and comply with the GDPR.

Is there scope for use in an employment context?

In light of the above, for employers to be entitled to rely on the Digital COVID Certificate as a method of ensuring a safe place of work, national legislation would be required to provide a legal basis for the Digital COVID Certificate to be used for this purpose.

As noted above, the Irish Government has introduced legislation to enable the Digital COVID Certificate to be used to facilitate safe indoor service in bars and restaurants due to concerns regarding the high risk of transmission of Covid-19 in these settings. In these circumstances, currently only a Digital COVID Certificate showing proof of vaccination or recovery from Covid-19 is applicable, and certificates demonstrating proof of a negative test result are not accepted (although this may be subject to change in the future).

The Health Amendment Act provides that an indoor operator may not permit access to their indoor premises to a person other than a 'permitted person' (as defined under the Health Amendment Act). The legislation further provides that an adult person may demonstrate that they are a 'permitted person' by providing evidence of 'proof of immunity' through vaccination or recovery from Covid-19. The Health Amendment Act states that the Digital COVID Certificate may be used as such proof of immunity.

There has been no suggestion that the Government intends to introduce legislation to allow use of the Digital COVID Certificate in an employment context as yet. Given the rapid pace of development in this area, it is possible that such legislation may ultimately be introduced. However, as set out above in connection with Article 5(1)(c) and the requirement for data minimisation, it may be difficult for the Government to find that proof of immunity from Covid-19 through vaccination or recovery from Covid-19 is necessary to facilitate safe access to workplaces generally.

If any legislation were to be introduced to facilitate use of the Digital COVID Certificate in this context, it would be more likely to be applied on a sector specific basis, where a high risk of transmission has been identified that cannot be mitigated by the standard prevention measures such as social distancing or masks.

Conclusions

There are a number of data protection considerations that an employer must take into account when developing a plan to return employees to their office workplaces safely.

For vaccination status data, the employer will need to carefully consider the nature of the work it conducts, its industry and its need for employee attendance as against how it can ensure safety for employees who do need to return to the office (potentially without seeking vaccination status data).

An employer considering seeking this information must also consider how to facilitate employees who

may not wish to provide it. Further, the picture for the use of the Digital COVID Certificate in office settings looks like it would require legislation at Irish level in order to be permissible and, at the time of writing, such legislation had not been proposed and is considered unlikely.

When weighing up data protection and ensuring employee safety, finding an appropriate balance will always depend on the purpose of the processing. This picture is informed by the nature of the business, the need for employees to physically be present in the workplace and the public health position. We have set out an analysis of some of these factors here, however, the past 18 months have shown how quickly priorities can shift in different directions. In the midst of this uncertainty, one certain point is that data protection will remain a significant issue for employers to consider when designing a workplace safety plan.

Aoife Mac Ardle

Lisa Leonard

McCann FitzGerald

aoife.macardle@mccannfitzgerald.com

lisa.leonard@mccannfitzgerald.com
