Commercial.
Decisive.
Expert.

Vaccines and data protection: what employers need to consider

It is hoped that the current vaccination programme which is being rolled out not only releases the UK lockdown but also allows those employers who wish to get their employees back into their usual workplaces and offices to do so.

We have received a number of enquiries about the steps an employer needs to take if it wishes to collect data on who and who has not received a covid 19 vaccination.

We would like to emphasise that it is our view that the government requirements in respect of ensuring workplaces are covid secure will be in place for some considerable time and that simply collecting data on who has and has not within your workforce been vaccinated will not be a green light to relax other safety measures.

ICO guidance

The Information Commissioners Office ("The ICO") has issued guidance on keeping data in respect of employee covid test results and data on employees who have suffered from covid symptoms. The ICO makes it clear that asking for this data, and the internal safety steps you must put in place to protect this data, must be reasonable, fair and proportionate.

It is unclear if further guidance on keeping data in respect of who has and has not had a covid 19 vaccine within a company will be issued by ICO. Our view is that if any such guidance is issued it will detail that additional measures are required as data on a persons vaccine status is data concerning their health which is classified as Special Category Data under the GDPR regime.

Why are you collecting the vaccine data?

When deciding whether to collect data concerning your employee's vaccination status it is crucial you ask is "is the data we are collecting necessary?"

There are a number of other vaccines individuals do or do not choose to have for a number of different diseases. Most employers do not currently ask for this data. It is vital therefore some thought is given as to whether collecting this data serves a necessary purpose.

Whilst the clinical trials show that a covid 19 vaccine prevents many people becoming seriously ill it is as yet unknown as to whether the current vaccines prevent transmission of the disease. It is in this context employers need to ask themselves whether keeping this data does make your

workplace any safer. This is along with the fact a great many employees are working from home and not coming into contact with their colleagues. You may be able to keep your workplace as safe as possible without collecting this data.

You may however form a view that collecting such data is necessary because of your business needs. For example:

- You may have an employee that is required to travel abroad as part of their duties, and other countries may implement rules for those who have not been vaccinated;
- You may be subject to restrictions about entering customer/client sites for those not vaccinated;
- Your work may involve close contact with vulnerable people;
- You may have employees who are clinically extremely vulnerable, so could be at grave risk if they are being asked to work in close contact with others.

What data should I hold and how long for?

If you form the view that it is necessary for your business to hold data about your employees vaccination status we would suggest only storing whether an employee has had a vaccination or not and if they have received one the date of doing so.

Similarly, it is important any such data is stored for as shorter period as possible. We envisage this will change as the pandemic develops. As our understanding of covid 19 changes it may be the case that the vaccine only gives protection for a limited amount of time. So, for example, if in the future it is discovered vaccination immunity lasts six months we would not recommend this data is stored for a period much longer than 6 months.

It is also important that you are clear and open with your staff about the data that you require and how it will be stored.

What steps do I need to take to ensure data protection compliance?

We would recommend taking two steps to achieve compliance. The **first step** is conducting a **data impact assessment.**

This impact assessment should be in writing and cover the following areas:

a. The purpose for which you are processing the data;
b. Why is it necessary and proportionate to have the vaccine data and the benefits of holding it;
c. A description of the data that will be held;
d. The legal basis you have for holding the data. As the information relating to any vaccination status amounts to "special category data" not only must you identify one or more of the general valid bases for processing the data but also a separate basis under Article 9 of the GDPR. These lawful bases could include:
    i. For the purposes of complying with the employers' legal obligations to ensure, so far as is reasonably practicable, the health, safety and welfare at work of your employees under the Health and Safety at Work Act 1974;
    ii. For the purposes of complying with your implied contractual obligations in order to protect health and safety at work;
    iii. For the purposes of protecting the employee's vital interests and those of others;
    iv. For the purposes of carrying out obligations in the field of employment law;
    v. For the purposes of assessing working capacity on health grounds.
e. How employees will be informed about the data that is being held;
f. Details of if the data will be shared with other organisations and why;
g. Explain how long the data will be held for and why;
h. Detail the steps you will take to ensure the data is accurate and will be kept up to date;
i. How employees will be made aware of their data rights and how any such requests will be dealt with;
j. How the data will be stored and the technical and organisational measures that will be in place to ensure it is secure. It is important to be transparent about who will see and hold the data.
k. Identify the countries the data will be stored in.

Once you have conducted this impact assessment you will have a written record of not only your decision making but also the basis on which you are holding this data and the security steps in place.

Commercial.
Decisive.
Expert.

This document will then need to be put into practice and the measures specified in it must be put in place. Remember to keep this document up to date. This is particularly important given the fluid and quick changing nature of the covid pandemic.

We then recommend a **second step which is updating your internal documents.** It maybe that you need to update your data protection policy and privacy notices to reflect the fact that you will be holding special category data. You should also ensure your retention guidelines specific the period for which you will hold the vaccine data and that you have the required data processor agreements with any third parties if sharing the information with other organisations.