OMBUDSMAN
CAYMAN ISLANDS

DATA PROTECTION GUIDANCE NOTE

Employee Vaccination Status Checks

A number of employers have signaled their intention to check whether their employees have been vaccinated against COVID-19.

In addition, the government has recently approved legislation to mandate that work permit holders must be vaccinated against COVID-19. We understand that checks on this will be incorporated into the existing work permit application process, with employees providing evidence to the employer, who will then submit that to WORC.

This guidance note explains the data protection implications of carrying out vaccination status checks on employees.

Establish a process for checking vaccination status

If you are considering checking your employees' vaccination status, you should be clear about what you are trying to achieve, and how asking people for their vaccination status helps to achieve this. You should create a written policy outlining how these checks will be done and what they will be used for.

The DPA is only one of many factors to consider when thinking about implementing vaccine status checks.

It would be advisable to also take into account:

- Employment law and your contracts with employees;
- Health and safety requirements; and
- Equality and human rights, including privacy rights.

If you decide to check your employees' vaccination status, you must do so in compliance with the eight data protection principles. More detailed guidance on each of these

principles can be found on our website: https://ombudsman.ky/data-protection-organisation/data-protection-principles

Fair and Lawful Processing

The DPA requires that the processing of personal data must be carried out in a fair and transparent manner.

In order for the processing to be considered fair and transparent, individuals must be told who is collecting the data (the data controller) and the purpose for collecting it. This information must be given to them promptly – usually by way of a written privacy notice.

a) Legal Basis

You must always have a legal basis to process personal data (see schedule 2 of the DPA). Where the law mandates that this data must be collected for work permit applications, then the legal basis is likely to be found in paragraph 3 of schedule 2 (processing under legal obligation). However, as with the other information that is collected as part of the work permit application process, the employer does not have an automatic right to use evidence of employees' vaccination status for its own purposes outside of the work permit application.

It has been suggested that employers could justify processing this personal data for their own purposes by relying on the requirement under the Labour Act (2021 Revision) that they should "ensure so far as is reasonably practicable the health, safety and welfare at work" of their employees. If seeking to rely on this, employers should consider the sector they work in, the kind of work their staff do and the health and safety risks in their workplace. It will not always be necessary to process personal data to meet this requirement. If this health and safety obligation does apply, then the legal basis in paragraph 3 would also apply here.

If neither of these apply, then you may have to consider paragraph 6 of schedule 2 (legitimate interests). You would have to balance your interests in collecting the data against the rights and freedoms of your employees.

b) Sensitive Personal Data

A person's COVID-19 vaccination status is medical information and is considered to be sensitive personal data under the DPA so you must ALSO meet a condition in schedule 3 of the DPA to be able to justify collecting this information.

For work permit applications, the condition in paragraph 2 of schedule 3 (performing an obligation imposed by law in connection with employment) would be likely to apply. The same condition would be used if the health and safety obligation mentioned above applies.

If no legal obligation exists, then it is difficult to identify a schedule 3 condition that could apply. Consent is rarely appropriate in an employment setting given the imbalance of power between the employer and employee, and it is unlikely to be valid in this instance.

If you cannot meet a schedule 3 condition, then you cannot collect this data.

Purpose Limitation

Personal data must only be used for purposes that are compatible with those for which it was collected in the first place. This means that you must be clear about the reasons for collecting this information, and you should only use it for purposes your employees would reasonably expect, and that have been specified in your written privacy notice or a similar communication.

Using information collected for the purpose of a work permit application for an incompatible purpose would be a breach of this principle.

Data Minimization

In accordance with the principle of data minimization, you should first consider all options that avoid the need to process personal data.

For example, if you are able to meet your health and safety obligations by putting in place measures such as social distancing, remote working and the wearing of appropriate PPE, then it will not be necessary to collect data on your employees' vaccination status.

If you must collect personal data to achieve your aims, then ensure that it is the bare minimum that is necessary. For example, you may just need to record that someone's vaccination status has been checked, rather than holding a copy of their vaccine certificate.

Other Principles

In addition to the requirements above, the data you collect must also be:

- accurate and up to date,
- stored securely,
- kept confidential with limited access to it, and
- kept only for as long as necessary.