DATA PROTECTION GUIDANCE NOTE

Vaccination and COVID Status Checks for Fitness Establishments

The latest COVID regulations[1] require owners and operators of gyms, fitness centres and other indoor fitness areas ("fitness establishments") to check vaccination certificates or PCR test results of any person (other than an employee) entering their premises. This guidance aims to help owners and operators to understand their obligations in relation to the Data Protection Act (DPA) when carrying out these checks.

A person's vaccination status or PCR test result is medical data and is therefore considered to be sensitive personal data under the DPA. Sensitive personal data is subject to stringent requirements under the DPA.

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 allow you to process personal data (see Schedule 2 of the DPA). In the case of vaccination status or PCR test results, the legal basis is likely to be found in paragraph 3 of schedule 2 (processing under legal obligation).

b) Sensitive Personal Data

A person's vaccination status or PCR test result is medical information and considered to be sensitive personal data under the DPA, so you must ALSO meet conditions in Schedule 3 of the DPA to be able to justify collecting this information. Paragraph 7(b) permits the

[1] http://gazettes.gov.ky/portal/pls/portal/docs/1/13108558.PDF

collection of this sensitive personal data on the basis that it is necessary for the exercise of any function (for example conduct checks of vaccination certification or PCR test results) under an enactment (for example under the COVID regulations).

Establish a process for checking vaccination status and PCR test results

Fitness facilities should create a written policy outlining how they will check vaccination status and PCR test results and a "privacy notice" explaining who is collecting the data and why it is being collected.

The COVID regulations do not explicitly require owners and operators of fitness establishments to retain a record of the checks they have made. You must decide if you feel that it is necessary to retain such records to prove compliance. A relevant question to ask is whether you could establish compliance in other ways.

If you decide to only conduct a visual examination of the certificate or test results, then the DPA would not likely apply because there would be no physical record of the data.

If the check is done electronically (for example, by electronically scanning the QR code displayed on the HSA health app), it would fall under the DPA - even if you do not keep a record of it. However, if you do not retain a record, you would only be required to explain why you are processing their data and what it will be used for.

If you decide to retain the vaccination certificate or PCR test result, 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

Purpose Limitation

Personal data must only be used for compatible purposes 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 customers and visitors would reasonably expect.

Data Minimization

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

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 or PCR test status has been checked, rather than holding a copy of their vaccination certificate or test results.

Other Principles

The data you collect must be:

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