

Bermuda employers turning to SafeKey to unlock return to new “normal”

Service area / [Employment, Pensions and Incentives](#)

Legal jurisdictions / [Bermuda](#)

Date / [September 2021](#)

On 9 September 2021, President Biden announced the development of an emergency rule to require all US employers with 100 or more employees (together over 80 million workers) to ensure their workforces are fully vaccinated or show proof of a negative COVID-19 test result at least once a week. The President characterised this initiative as one necessary to counter “*a pandemic of the unvaccinated*”, stating, “*This is not about freedom or personal choice. It’s about protecting yourself and those around you*”¹.

On 10 September 2021, Premier Burt characterised Bermuda’s approach to the pandemic thus far as “*a study in the emphasis of personal choice*”², and although the Government has implemented a ‘SafeKey’ vaccination/testing requirement for participation in certain activities, this requirement has not (yet) been extended to the country’s workforces. As “*there are no major proposed changes to the existing public health regulations at this time*”³, this briefing considers whether Bermuda’s employers can choose to enforce a workplace SafeKey regime in lieu of a legislated requirement.

What is ‘SafeKey’?

Under the ‘SafeKey’ regime, Bermuda’s Ministry of Health issues digital verification documents to individuals who have either been fully vaccinated against COVID-19 or have recently received a negative test result. Each verification document

¹ [See link](#)

² [See link](#)

³ *Ibid*

contains a unique QR barcode, or ‘SafeKey’, that can be scanned and authenticated by any member of the public. There are no charges associated with the use of the SafeKey software.

Vaccine-based SafeKeys currently remain valid for one month and may be renewed without the owner needing to meet additional requirements. Test-based SafeKeys remain valid for 72 hours following the test day and cannot be renewed.

SafeKeys are not available to individuals who: have acquired ‘natural immunity’ through contracting and recovering from COVID-19 but who would not otherwise meet the eligibility requirements above (vaccination/ recent test); are in isolation or quarantine; or are unvaccinated and have travelled in the preceding 14 days.

To verify an individual’s SafeKey, a user must visit the [verification webpage](#) on a capable device, such as a smartphone or tablet. The user will then, using the device’s camera, scan the SafeKey. The webpage will then display: confirmation of the SafeKey’s validity; the first and last initials of the SafeKey owner’s name; the day and month (but not year) of the SafeKey owner’s birthdate; and the expiry date of the SafeKey. The user must then check this information against photo identification presented by the SafeKey owner, such as a driver’s licence or passport.

OFFSHORE LAW SPECIALISTS

Where are SafeKeys required?

SafeKey legislation currently targets customers and service users of certain businesses, such as indoor bars, clubs, restaurants, gyms and sports clubs. SafeKeys are also required where groups have received a 'large group exemption' for gatherings exceeding the statutory cap (projected to be lowered from 50 to 20 persons).

The Government's [SafeKey Guidance](#) states that there are businesses and organisations that may "*voluntarily participate in the COVID-19 SafeKey Programme*". It is unclear, however, whether the Government intends for voluntary participation in the SafeKey programme to be limited to businesses and organisations that "*provide access to high risk services and activities for customers and service users*", and if so, which services and activities, besides those set out in the Regulations, should be classified as "*high risk*". It is clear, however, that no limitations have been placed on public access to the SafeKey verification software; conversely it appears that the verification software has been designed to be as widely accessible as possible.

Implementing an employee SafeKey requirement

Although there is currently no legal requirement for employees to participate in SafeKey verification, an employer's requirement of such participation may amount to a reasonable management instruction, and an employee's refusal to participate could become a disciplinary issue. Even though the requirement would apply to all employees equally employers should also consider whether such a policy could amount to indirect discrimination. This can occur where a policy has a disproportionate effect on a particular group who share a "protected characteristic" (i.e. disability) but cannot satisfy the requirement (i.e. vaccination) and suffer a disadvantage as a consequence (i.e. having to submit to regular testing in order to attend the office). It is possible that indirect discrimination can be justified if it is a proportionate means of achieving a legitimate aim (i.e. ensuring the health and safety of employees). The potential issue is whether there are any other less discriminatory means of achieving the same outcome (for example, simply maintaining existing COVID-19 safety protocols). In the circumstances, we consider implementing a Safekey policy is likely to be objectively justifiable on health and safety grounds (given the increased transmissibility of the Delta variant makes existing safety protocols less effective) and also potentially on economic grounds (as it may enable some employers to stay open rather than having to close due to regular outbreaks).

In practice, the employer needs to balance their reasons for enforcing a workplace SafeKey policy against the fundamental freedoms and rights of its employees.

This will not be a one-size fits all exercise. An employer should consider: the nature of its employees' roles; the location of the work done; the level of interaction between employees and members of the public; any risks identified by health and safety risk assessments; the employer's legal obligations relating to health and safety; and the potential for business interruption and/or reputational damage if the policy is not implemented.

An employer's implementation of a SafeKey policy would carry less risk than the implementation of a mandatory vaccination or testing regime as: SafeKey software is provided to the public by the Government, together with legislation and guidance; there is no need for the employer to handle or store employees' sensitive personal information; and such a policy would provide employees the choice of vaccination or regular testing, without needing to disclose this choice to the employer or colleagues.

Employers should consider the following points as part of any SafeKey implementation process:

Workplace risk assessment

The employer should undertake a workplace risk assessment of the ongoing risks relating to COVID-19 and identify the benefits of requiring employee SafeKey verification. The employer should consider whether other measures to minimise the risk of COVID-19 transmission could be more appropriate for the business. The employer should also consider whether to apply the policy to its entire staff or only to select employees (such as those in client facing roles).

It is important that the employer is able to clearly articulate why a SafeKey policy is the best course of action for the business. Possible justifications could include: the Government's endorsement of the tool; the need for updated staff and visitor safeguards to address the more transmissible Delta variant of the virus; fairness to colleagues who might otherwise be placed in quarantine due to contact tracing where an employee tests positive; the risk of severe disruption to the business if repeated shut downs are required; the flexibility of a SafeKey policy in comparison to a mandatory vaccination policy; and, where employees are unable to work remotely, the possibility of continued work in a safer working environment during a COVID-19 outbreak (such as is currently being experienced in Bermuda).

Informing and consulting with affected staff

The employer should adopt a clear and transparent communication strategy with affected employees regarding any proposal to implement a SafeKey policy. This should include open channels of communication to allow employees to come forward with questions and concerns. While there are no fixed parameters and the pandemic is fast moving, we would recommend that employers provide staff with some

Continued

lead-in time (possibly a week) before any SafeKey policy is introduced, to provide for employee discussion and test scheduling.

Practical considerations

Employers will need to develop a system for collecting and processing SafeKey information to ensure that employees are compliant. This could involve employees submitting SafeKey records electronically to a dedicated email address which is monitored by Human Resources. Alternatively, employers could adopt a self-certification approach whereby employees sign a declaration each week to confirm that they have a valid SafeKey and this could be enforced by random spot checks. Employers should also consider whether to offer to reimburse employees for any testing costs (that are not covered by insurance or Government) and whether to offer flexible testing arrangements such as home testing (if available).

Data protection considerations

As explained above, the SafeKey verification process will only reveal limited personal information about a SafeKey's owner which the employer will likely already have. Notably, the process does not reveal whether the SafeKey's owner is vaccinated or unvaccinated, or whether the SafeKey's owner is or has ever been COVID-19 positive. However, where the employer chooses to keep a note of an employee's SafeKey data, there is a chance that the employee's vaccination status may be inferred from their SafeKey expiration dates.

Any information relating to vaccination or COVID-19 status will be "*sensitive personal information*" for the purposes of Bermuda's Personal Information Protection Act 2016 (not yet in force). We consider that employers can process and use this data on the same basis as other employee health information: namely, where the processing is either: necessary for performing obligations or exercising rights which are imposed or conferred by law; or otherwise necessary in the context of the employment relationship. As with other sensitive personal information, employers should adopt appropriate data security measures, and should only keep records of such information for as long as is reasonably necessary.

Disciplinary action for non-compliance

The employer should consider how it will address noncompliance, particularly where employees face significant difficulty in meeting SafeKey renewal obligations; some employees cannot be vaccinated due to disability or religious belief, and testing may be inaccessible and/or prohibitively expensive. While refusal of a reasonable SafeKey policy may be grounds for disciplinary action, an employer may wish to consider flexibility where possible, given the emotive nature of this issue and current lack of a Government requirement for SafeKey use in the workplace.



FIND US

Carey Olsen Bermuda Limited
Rosebank Centre 5th Floor
11 Bermudiana Road
Pembroke HM 08
Bermuda

T +1 441 542 4500
E bermuda@careyolsen.com



FOLLOW US

Visit our employment, pensions and incentives team at careyolsen.com



PLEASE NOTE

Carey Olsen Bermuda Limited is a limited liability company incorporated in Bermuda and approved and recognised under the Bermuda Bar (Professional Companies) Rules 2009. The use of the title "Partner" is merely to denote seniority. Services are provided on the basis of our current terms of business, which can be viewed at: www.careyolsen.com/terms-business

This briefing is only intended to provide a very general overview of the matters to which it relates. It is not intended as legal advice and should not be relied on as such. © Carey Olsen Bermuda Limited 2021.