Cases 202100552/553

Enforcement Order

CIBC First Caribbean International Bank (Cayman)

21 March 2023

SUMMARY

In September 2021 employees of CIBC First Caribbean Bank (Cayman) (the Data Controller) were informed that a new policy was being implemented, requiring them to provide proof of Covid-19 vaccination or weekly negative PCR test results. Employees who failed to comply were required to go on unpaid leave. Two employees complained to the Office of the Ombudsman, alleging violations of the Data Protection Act (2021 Revision) (DPA).

The Ombudsman investigated the allegations and drew the following conclusions:

- Employees were properly informed of the purpose for the data gathering, as required under the first data protection principle.
- The purpose of the processing was legitimate and explicitly specified, and there was no violation of the second data protection principle.
- The data was not kept for longer than required for the stated purpose, and there was no violation of the fifth data protection principle.

The Ombudsman however found the following violations:

- The Data Controller did not have a legal basis (data processing condition) for the processing, as required by the first data protection principle and Schedules 2 and 3;
- The processing of the data relating to the data subjects' vaccination status and PCR testing was excessive as it was not necessary to meet the Data Controller's obligations under the Labour Act, which was the legal basis relied on.
- A reminder email to employees who had not yet provided their data, sent without use of BCC, risked inferences to be made about the individuals' health and/or medical status, and therefore violated the seventh data protection principle.

The processing of personal data that lead to the complaints is no longer in practice, and therefore no corrective action is required.

The Ombudsman required the Data Controller to demonstrate how it is meeting the requirements of the eighth data protection principle, which regulates the international transfer of personal data, as this was insufficiently explained by the data controller.

A. BACKGROUND

[1] On 6 September 2021 employees of the Data Controller were told that a new policy (the Policy) was being implemented, requiring them to provide proof of Covid-19 vaccination status by 14 October 2021, or provide weekly negative test results from a Polymerase Chain Reaction (PCR) test, with the costs for testing being borne by the employee. Failure to provide either proof of vaccination or a negative PCR test result would require the employee to go on unpaid leave until a negative test result or proof of vaccination was provided.

[2] On 25 October 2021 two complaints were raised under section 43 of the DPA against the Data Controller, the complainants' employer, relating to the processing of the complainants' personal data in accordance with the Policy.

[3] The Policy was subsequently adjusted, including the introduction of Lateral Flow Testing (LFT).

[4] The complainants made the following allegations:

a) The Data Controller was using the personal data of the complainants in a way they did not want them to.
b) The Data Controller had failed to keep the data secure.
c) No adequate explanation was provided for the purpose or the reasoning of the new Policy, or for the processing of medical information such as the weekly PCR test results.
d) It was not explained what law authorized the Data Controller to request the data from the data subjects.

e) Insufficient information was provided to explain how the processing of the vaccination status data would be handled and how many people would have access to it. This also raised questions about the potential transfer of the data abroad.
f) No explanation was provided as to the retention of the data.

B. CONSIDERATION OF ISSUES

[5] I have considered the complaints and the responses received from the Data Controller under the relevant data protection principles in Schedule 1 of the DPA.

I. First data protection principle – fairness and legal basis:

[6] The first data protection principle involves questions on the fairness and legal basis for the processing. It states:

> *1. Personal data shall be processed fairly. In addition, personal data may be processed only if -*
>
> > *(a) in every case, at least one of the conditions set out in paragraphs 1 to 6 of Schedule 2 is met; and*
> > *(b) in the case of sensitive personal data, at least one of the conditions in paragraphs 1 to 10 of Schedule 3 is also met.*

[7] Part 2 of schedule 1 of the DPA further explains certain aspects of the first principle:

> ***First principle: source***
> *1. (1) In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to —*
>
> > *(a) the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed; and*

> *(b) whether the information contained in the personal data has previously been made public as a result of steps deliberately taken by the data subject.*
>
> *(2) Subject to paragraph 2, for the purposes of the first principle, personal data are prima facie to be treated as obtained fairly if they consist of information obtained from a person who is required to supply it by or under an enactment or by a convention or other instrument imposing an international obligation on the Islands.*
>
> ***First principle: specified information at relevant time***
> *2. For the purposes of the first principle personal data shall not be treated as processed fairly unless the data subject has, as soon as reasonably practicable, been provided with, at a minimum —*
>
> *(a) the identity of the data controller; and*
> *(b) the purpose for which the data are to be processed.*

Fairness

[8] The complaints raise the question whether the employees were adequately informed of the purpose of the processing, pursuant to paragraph 2 of Schedule 1.

[9] The Data Controller informed its employees of the new Policy on 6 September 2021, putting the question of vaccination in the broader context of the Islands' imminent plans to lift Covid quarantine measures. The Data Controller referenced discussions with the Cayman Islands Bankers' Association on the protection of clients and third-party providers, and stated that it intended to "secure the safety of every employee".

[10] In view of the limited legal requirements for informing data subjects specified in paragraph 2 of part 2 of Schedule 1 (quoted above), this notification was adequate as it contained the two elements required: the Data Controller's identity and the purpose for which the data was collected.

[11] The DPA does not require data controllers to notify data subjects how long personal data will be kept. See below for more on the retention of data in the discussion of the fifth data protection principle.

[12] There is no suggestion that the method of obtaining the data was based on deception or was misleading the data subjects, as addressed in the first paragraph of part 2 of schedule 1.

[13] **Consequently, the Data Controller's email of 6 September 2021 to its employees met the fairness requirements of part 2 of Schedule 1 of the DPA.**

Legal basis

[14] The first data protection principle requires that at least one of the conditions in Schedule 2, and in the case of sensitive personal data (as defined in section 3 of the DPA) also one of the conditions in Schedule 3, is met. The personal data in question consisted of individuals' vaccination status and results of medical tests. Since these were medical and health-related data, they consisted of sensitive personal data, and Schedule 2 as well as Schedule 3 applied.

[15] The Data Controller relied on section 58 of the Labour Act (2021 Revision), which states:

> ***General duty of employers***
> *58. Every employer shall ensure so far as is reasonably practicable the health, safety and welfare at work of that person's employees.*

[16] The Data Controller therefore appeared to rely on paragraph 3 of Schedule 2, and paragraph 2 of Schedule 3, as follows:

> ***Schedule 2:***
> ***Processing under legal obligation***
> *3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.*
>
> ***Schedule 3:***
> ***Employment***
> *2. The processing is necessary for the purposes of exercising or performing a right, or obligation, conferred or imposed by law on the data controller in connection with the data subject's employment.*

[17] Both of these processing conditions require a consideration of whether the processing is necessary for the stated purpose(s). According to the UK Information Commissioner, necessity and proportionality in a data protection context aim to:

> *… consider that our processing achieves the purposes set out … and does not go beyond what is reasonably necessary to achieve these purposes.*
> *…*
> *We ensure data minimisation and proportionality by only asking for data that we need for a current specified purpose.*[1]

[18] As well, the European Data Protection Supervisor has clarified the meaning of "necessity" as follows:

> *Necessity implies the need for a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal.*[2]

[19] The Data Controller explained that it did not conduct a formal written analysis for consideration by senior management before issuing the Policy. In considering necessity, the Data Controller's implied position was that the processing described in the Policy was, indeed, necessary to achieve the stated purpose, which was to secure the safety of every employee. This position seems untenable in light of the existence of options that were less intrusive in respect of the rights of the individuals, such as the use of PPE, social distancing, working remotely, etc.

[20] The Department of Labour & Pensions (DLP) issued guidance on Covid vaccinations and the duty of employers under section 58 of the Labour Act in August 2021.[3] This document does not appear to support the position of the Data Controller, in particular where disciplinary

---

[1] Information Commissioner's Office (UK), *Sample Data Protection Impact Assessment Online Retail - Step 4: Assess necessity and proportionality*, at: https://ico.org.uk/for-organisations/childrens-code-hub/sample-data-protection-impact-assessment-online-retail/step-4-assess-necessity-and-proportionality/

[2] European Data Protection Supervisor, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*. 11 April 2017, p.4., at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf

[3] Department of Labour & Pensions, *Coronavirus (COVID-19) – General Guidance Document re The COVID-19 vaccine,* 9 August 2021, at: http://dlp.gov.ky/portal/page/portal/dlphome/publications/dlp-general-guidance-document-regarding-covid19-vaccine

action or dismissal is concerned, which was the effective consequence of non-compliance by the employees.

[21] The argument for "necessity" of the Policy is also weakened by the stated aim of ensuring that staff are "covid negative" to provide a safe environment. Targeting the PCR testing scheme at non-vaccinated individuals was unfair, given that being vaccinated does not ensure that people are "covid-negative", and therefore, it should have been implemented for all staff. This would have eliminated the need to request, analyze and store the vaccination status of any individuals. The subsequent switch to LFT appears to acknowledge this, although the later policy continued to contain more restrictive provisions for unvaccinated individuals.

[22] It seems difficult for the Data Controller to justify the requirement that staff had to notify them of their test results. The law at the time placed a legal obligation on individuals who had tested positive to notify this to Public Health/the Chief Medical Officer, and any positive diagnosis would be handled in accordance with Public Health protocols. However, there was no need for the Data Controller to obtain, analyze and store the test results of any of its employees under either of the testing regimes (PCR or LFT). They would inevitably be made aware of any positive tests when the employees called in sick, but this is a separate processing activity with a separate legal basis.

[23] **In conclusion, I find that the Data Controller failed to meet the requirements of the first data protection principle in relation to the legal bases for processing in Schedules 2 and 3 of the DPA.**

II. Second data protection principle – purpose limitation:

[24] The second data protection principle states:

> ***Second principle***
> *2. Personal data shall be obtained only for one or more specified lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes*.

[25] **The purpose of the processing, itself, was explicitly specified and legitimate, and compliance with the vaccination and testing Policy was compatible with this purpose. Therefore, there was no violation of the second principle.**

III. Third data protection principle – data minimization:

[26] The Third data protection principle states:

> ***Third principle***
> *3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are collected or processed.*

[27] The Data Controller was not clear in some of its responses as to what personal data was actually being processed under the Policy, possibly because of a misunderstanding of what constituted a "record". Initially, they claimed not to be holding vaccination certificates or test results. Later, they confirmed that they held vaccination cards and PCR test results on a network drive.

[28] According to the Data Controller the risk factors of all staff varied only slightly, and no distinction could be made between different categories of staff. Frontline staff were dealing with external clients, but all staff shared the same spaces such as bathrooms, lunch room, etc. Therefore, the approach was the same for all staff.

[29] However, as explained above, the data were not "necessary" to meet the Data Controller's obligations under the Labour Act, which was the stated legal basis for processing.

[30] **Therefore, I find that the processing of the data (including collecting, analyzing, storing, etc.) relating to the data subjects' vaccination status and PCR testing was excessive, and it violated the third data protection principle.**

IV. Fifth data protection principle

[31] The fifth data protection principle states:

Fifth principle

5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

[32] In response to our queries the Data Controller confirmed that the personal data were retained for only one month, in an electronic format. They also clarified that these data were not kept on employee files, and were not shared.

[33] **Consequently, I find that there was no violation of the fifth principle.**

IV. Seventh data protection principle

[34] The seventh data protection principle states:

Seventh principle

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

[35] The Data Controller sent a reminder email to seven employees who had not yet provided their vaccination status, asking them to submit their data by 14 October 2021. The email was sent without using BCC, so that all recipients could see the other recipients's email addresses and names. The complainants expressed concerns about this, as this approach could potentially constitute a data breach involving sensitive personal data in the form of medical data.

[36] The Data Controller did not believe the vaccination status of these seven employees could be reasonably inferred from this email. However, it should have been more aware of the other inferences that could have been drawn. It is noteworthy that a recent decision of the UK Information Commissioner, in a different context, made it clear that an issue arises with

potential inferences leading to the profiling of individuals, irrespective of whether the inferences are correct or not.[4]

[37] The Data Controller's approach in not using BCC in the email represented a risk, particularly since some of the individuals had not been vaccinated. This approach could have facilitated the profiling of the seven individuals, and should be avoided in the future in respect of data that could lead to inferences (whether correct or not) about individuals' health and/or medical status.

[38] **Therefore, I find that the reminder email sent without use of BCC was a violation of the seventh data protection principle.**

V. Eighth data protection principle

[39] The eighth data protection principle states:

> ***Eighth principle***
> *8. Personal data shall not be transferred to a country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data*.

[40] We received contradictory accounts of whether employees' data was sent abroad or not. One complainant stated that she was told to send her information to the Data Controller's HR department, which she and some others interpreted as the HR department in the Bahamas, while employees in another section of the office had their HR department in the Cayman Islands. According to this version, the data were sent to the Bahamas and were then returned to the Cayman Islands for further action.

[41] The Data Controller initially contradicted this version of events, stating that individual employees may have misunderstood where to send their information, but that it was the

[4] See: Information Commissioner's Office (UK), *Data Protection Act 1998. Supervisory Powers of the Information Commissioner. Enforcement Order. Easy Life Limited*. 6 October 2022, at: https://ico.org.uk/media/action-weve-taken/enforcement-notices/4021803/easylife-limited-en-reg-21-20221004.pdf

controller's intention that the information should be sent to the local HR department in the Cayman Islands. The instructions provided to staff seem to only refer to "sending the information to HR" without specifying whether this was in the Bahamas or the Cayman Islands. The Data Controller confirmed that some employees sent their data to the HR officer in the Bahamas, but it was immediately returned.

[42] In response to our repeated queries, the Data Controller eventually corrected its previous statements as follows:

> *At the time of the introduction of the vaccination policy, HR at FirstCaribbean International Trust Company (Bahamas) Limited ("Bahamas Trust Co.") was responsible for the staff of the FirstCaribbean International Bank and Trust Company (Cayman) Limited ("Cayman Trust Co.").*
>
> *… in September 2021, the HR-related matters for the Cayman Trust Co. were the responsibility of the Senior Human Resources Consultant, Bahamas Trust Co. who was in the Bahamas. This arrangement was put in place following the exit of the Cayman Trust Co. Senior Human Resources Consultant in October 2020.*
>
> *A year later, on 31 October 2021, the Consultant in the Bahamas exited the organisation and the HR responsibilities for the Cayman Trust Co. were assigned to the Head, Human Resources – Cayman, BVI and the Cayman Trust Co. in addition to the HR-related matters for FirstCaribbean Bank, Cayman and FirstCaribbean Bank, BVI.*

[43] We pressed the Data Controller on its international transfer of personal data, asking what measures were in place in regard to compliance with the eighth data protection principle. In its response the Data Controller indicated that it had "security control measures for the protection, storage and transfer of personal data at rest and in transit", as well as for "the protection of its technology infrastructure". The Data Controller also stated that "information security/cybersecurity and the protection of [its] information is governed by the… Information Security/Cybersecurity Risk and Technology Governance Policy", quoting several paragraphs.

[44] These responses appear to address the demands of the seventh data protection principle, rather than those of the eighth principle. The eighth principle relates to the adequacy of the protection of the rights and freedoms of the data subjects when data are transferred internationally, not only or primarily to the security of the data. The DPA prohibits such transfers unless the data controller can show that the overseas jurisdiction offers adequate protection. Paragraph 4, part 2 of schedule 1 of the DPA states:

> ***Eighth principle: what is adequate protection in foreign country***
> *4. For the purposes of the eighth principle, an adequate level of protection is one that is adequate in all the circumstances of the case, having regard, among other things, to —*
> *(a) the nature of the personal data;*
> *(b) the country or territory of origin of the information contained in the data;*
> *(c) the country or territory of final destination of that information;*
> *(d) the purposes for which and period during which the personal data are intended to be processed;*
> *(e) the law in force in the country or territory in question;*
> *(f) the international obligations of that country or territory;*
> *(g) any relevant codes of conduct or other rules that are enforceable in that country or territory, whether generally or by arrangement in particular cases; and*
> *(h) any security measures taken in respect of the data in that country or territory.*

[45] Schedule 4 of the DPA provides a number of derogations from the eighth principle, and the eighth principle is further explained in our online guidance.[5]

[46] Barring a derogation, the Data Controller should have demonstrated how its international transfer of personal data meets the requirements of the eighth data protection principle, namely how it "ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

[5] https://ombudsman.ky/data-protection-organisation/data-protection-principles/eighth-data-protection-principle-international-transfers

[47] **Consequently, the Data Controller has not demonstrated whether or how it is meeting the requirements of the eighth data protection principle.**

C. FINDINGS AND DECISIONS

[48] Under section 45(1) of the DPA, for the reasons explained above, I make the following findings and decisions:

First data protection principle:

a) The Data Controller's email of 6 September 2021 to its employees met the fairness requirements of part 2 of Schedule 1 of the DPA.

b) The Data Controller did not have a valid condition/legal basis for the processing under the first data protection principle and Schedules 2 and 3 of the DPA.

Second data protection principle:

c) The purpose of the processing, itself, was explicitly specified and legitimate, and compliance with the vaccination and testing policy was compatible with this purpose. Therefore, there was no violation of the second principle of the DPA.

Third data protection principle:

d) The processing of the data (including collecting, analyzing, storing, etc.) in relation to the data subjects' vaccination status and PCR testing was excessive, since those data were not "necessary" to meet the Data Controller's obligation under the Labour Act, which was the stated legal basis for processing. As such, processing the data was excessive, and in violation of the third data protection principle of the DPA.

Fifth data protection principle:

e) There was no violation of the fifth principle of the DPA.

Seventh data protection principle:

f) The reminder email sent without use of BCC was a violation of the seventh data protection principle of the DPA.

Eighth data protection principle:

g) The Data Controller has not adequately explained how it is meeting the requirements of the eighth data protection principle of the DPA in transferring personal data internationally.

[49] In similar data processing activities in the future, I require the Data Controller to ensure that:

a) It meets the requirements of the first data protection principle and Schedules 2 and 3 when processing sensitive personal data, i.e. that its processing of sensitive personal data meets at least one condition/legal basis in Schedule 2, as well as one in Schedule 3 of the DPA.
b) it does not process personal data excessively, and ensures that all processing is necessary to meet the requirements of the applicable legal basis.
c) it uses BCC when sending emails from which inferences can be made about individuals, leading to the potential profiling of individuals, whether correct or not.

[50] Since the Data Controller has not demonstrated how it is meeting the requirements of the eighth data protection principle, and since it appears that the Data Controller is transferring personal data to jurisdictions that do not have an adequate level of protection (including, but not limited to, the Bahamas), the Data Controller has 45 days to explain and provide documentation for review by my office, on the following:

a) the precise nature of the Data Controller's international transfers of personal data to any non-adequacy countries;
b) whether the Data Controller considers that any derogations apply to any of its international transfers, and if so, which derogations apply to which transfers and how they apply (schedule 4 DPA);
c) whether the Data Controller has any safeguards in place, e.g. standard contractual clauses (GDPR-based SCCs may be acceptable), if so, what applicable provisions are in place – please provide copies;
d) whether the Data Controller considers that its international transfers are deemed to provide adequate safeguards as a result of an adequacy self-assessment (schedule 1, part 2(4)), if so, please provide a copy of the self-assessment; and,

e) any other information the Data Controller considers relevant to its compliance with the eighth data protection principle.

[51] Under section 47 of the Act, a person who receives an enforcement order under the DPA may, within 45 days of receipt and upon notice to the Ombudsman, seek a judicial review of the Order to the Grand Court.

Sharon Roulstone
Ombudsman