REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

ODPC COMPLAINT NO. 1958 OF 2024

CATHERINE KAINYU MURITHI .....COMPLAINANT

-VERSUS-

BECTON DICKINSON AND COMPANY

T/A BD EAST AFRICA.....1ST RESPONDENT

SAFARICOM PLC.....2ND RESPONDENT

DETERMINATION

(Under Section 8(1)(f) and 56 of the Data Protection Act, 2019 and Regulation 14 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021)

A. INTRODUCTION

1. The complaint filed on 27th November 2024, concerns the unauthorized disclosure of the Complainant's copy of national identity card by the 1st Respondent to the 2nd Respondent, as well as the Respondents' handling and processing of the Complainant's personal data for an alleged unauthorized mobile number account/sim card ownership transfer without consent.

B. LEGAL BASIS

2. Article 31(c) and (d) of the Constitution of Kenya provides for the right to privacy. Consequently, as an effort to further guarantee the same, the Data Protection Act, 2019 (hereinafter known as 'the Act') was enacted.

3. The Office of the Data Protection Commissioner (hereinafter as 'this Office' and/or 'the Office') was established pursuant to Section 5 of the Act and is mandated with the responsibility of regulating the processing of personal data; ensuring that the processing of personal data of a data subject is guided by the principles set out in Section 25 of the Act; protecting the privacy of individuals; establishing the legal and institutional mechanism to protect personal data and providing data subjects with rights and remedies to protect their personal data from processing that is not in accordance with the Act.

4. Section 8(1)(f) of the Act provides that the Office can receive and investigate any complaint by any person on infringements of the rights under the Act. Furthermore, Section 56(1) of the Act provides that a data subject who is aggrieved by a decision of any person under the Act may lodge a complaint with the Data Commissioner in accordance with the Act.

5. This determination is premised on the provisions of Regulation 14 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 (hereinafter as 'the Enforcement Regulations') which states that the Data Commissioner shall, upon the conclusion of the investigations, make a determination based on the findings of the investigations.

C. BACKGROUND OF THE COMPLAINT

6. This Office received a complaint from the Complainant on 27th November 2024. The complaint was lodged pursuant to Section 56 of the Act and Regulation 4 of the Enforcement Regulations by the Complainant, who was an aggrieved data subject.

7. Pursuant to Regulation 11 of the Enforcement Regulations, the Office, notified the Respondents of the complaint filed against it *vide* letters dated 11th December 2024 and referenced ODPC/CONF/1/5/VOLII(364) and ODPC/CONF/1/5 /VOL II(365) respectively. In the Notification of the Complaint, the Respondents were informed that if the allegations by the Complainant were true, they were in violation of various provisions of the Act. Further, the Respondents were asked to provide this Office with the following: -

a. A response to the allegations made against it by the Complainant;

b. A contact person who can provide further details as regards the complaint.

c. Provide any relevant materials or evidence in support of your response.

d. The legal basis relied upon to process with the Complainant's data.

e. Evidence of whether the Complainant consented to the sharing of his personal data with third parties.

f. The mitigation measures adopted or being adopted to address the complaint to the satisfaction of the Complainant if any.

g. The mitigation measures adopted or being adopted to ensure that such occurrence mentioned in the complaint do not take place again.

h. Any other relevant information the Respondents wishes the Office to consider.

8. The 1st Respondent responded to the Notification of Complaint letter *vide* a letter dated 3rd February 2025 while the 2nd Respondent responded on the 27th December 2024.

9. The Complainant issued a rejoinder to the 1st Respondent's response on the 25th January 2025 and to the 2nd Respondent's response on the 10th January 2025 respectively.

10. This determination is therefore a result of analysis of the complaint as received, the response by the Respondent and investigations conducted by the Office.

D. NATURE OF THE COMPLAINT

11. The complaint filed on 27th November 2024, concerns the unauthorized disclosure of the Complainant's copy of national identity card by the 1st Respondent to the 2nd Respondent, as well as the Respondents' handling and processing of the Complainant's personal data for an alleged unauthorized mobile number account/sim card ownership transfer without consent.

E. SUMMARY OF RELEVANT FACTS AND EVIDENCE ADDUCED

i. THE COMPLAINANT'S CASE

12. The Complainant alleges that pursuant to an employment contract dated 27th and 28th September 2021 respectively, the Complainant was employed by Becton Dickinson and Company t/a Becton Dickinson (BD) East Africa effective 16th August 2021 as the Global Health Leader for Africa.

13. Prior to the start date, BD's Office Administrator, reached out to the Complainant on 3rd August 2021 and requested for various personal documents particulars of which included: marriage certificate, birth certificates of the Complainant's children, copy of the Complainant's national identity card, copy of the Complainant's passport, copy of the Complainant's KRA PIN Certificate, NSSF and NHIF Number and her banking details.

14. Although BD's Office Administrator did not inform the Complainant of the use to which her personal data was to be put, the legitimate expectation was that the personal data was relevant for the purposes of verifying the accuracy of the Complainant's details, supporting and fulfilling the employment contract as a HR requirement during the pre-employment application process.

15. In addition, the Complainant had a legitimate expectation that BD would not disclose her personal information without consent. The Complainant therefore shared copies of her personal data with BD. Notably, the Complainant's employment contract did not include any information on how her personal and sensitive data would be handled and for what purposes both during her tenure and or post-employment.

16. Soon after the Complainant had joined employment, BD's Office Administrator reached out and informed her that in order to register her post-paid personal Airtel number +2547******** under the BD account, she needed to terminate airtel SIM card services so that the mobile number +2547******* could be registered with a new carrier which was Safaricom under the BD account. Consequently, +2547******* became the Complainant's official communication number that BD was being billed for by Safaricom during the Complainant's employment tenure.

17. On 30th September 2024, BD East Africa issued the Complainant with a termination letter due to what they termed as 'redundancy' effectively ending the employment contract between BD and the Complainant. Subsequently on the 18th August 2024, the Complainant also received a clearance form with a check list of properties she needed to return to BD as well as some actions items, one of the actions being the deactivation of the BD billed SIM card. This clearance form did not have any listed action or requirement for BD to register the Complainant's personal line under the Complainant's Identity after deactivation of the BD billed SIM card.

18. It came to the Complainant's attention that on 3rd October 2024 and 4th October 2024 after she had ceased being an employee of BD East Africa, the Office Administrator acting on behalf of Becton Dickinson and company t/a BD East Africa without the Complainant's consent went ahead and shared her national ID card copies containing personal and sensitive information with Safaricom's representative-B**** O****** in order to facilitate the registration of her private mobile number/transfer of the same to the Complainant's national ID after the BD billed number had been terminated from the BD account. An action that was completely unlawful, unconstitutional and with no legitimate purpose.

19. In an email dated 3rd October 2024 under the subject, 'Exit Notice-Catherine Murithi-+254 7********,' BD through the Office Administrator informed Safaricom as follows: "*Greetings B****, I hope you are doing well. Please note that Catherine Murithi +254 7******** is no longer with BD. Please help transfer her line above including accumulated bonga points from the BD account to her personal use, effective immediately. Her ID number is 2********. Kindly let us know once actioned and in case you have any questions.*" This communication not only authorised the termination of the BD billed SIM card on the basis that the Complainant was no longer a BD employee but also instructed Safaricom to transfer the Complainant's line from the BD account to her personal account.

20. The Complainant states that asking Safaricom to terminate or deactivate the BD billed line was in order and was the only administrative action that BD was

supposed to execute. However BD went ahead to unlawfully share the Complainant's National ID card details and copies to third parties (Safaricom) including cross-border transfer of her data to persons not known to her (L*** M*********; finance department, BD, South Africa and K***** R******* (Trainee,BD South Africa) without the Complainant's consent.

21. Further BD acted on the Complainant's behalf and went ahead to collude with Safaricom officials to register her private number rather transfer the number to her ID on her behalf without her consent. By email correspondence dated 03/10/2024 addressed to BD's Office Administrator, Safaricom through B**** O****** requested BD to share copies of the Complainant's National Identification Card as a prerequisite for transferring the terminated BD billed number to the Complainant's National Identity.

22. According to Safaricom these copies were shared by BD in a separate mail that the Complainant was not party to thus enabling Safaricom to transfer the terminated BD billed number to the Complainant's identity, register the transferred BD billed number to the Complainant's Identity card under the Safaricom's prepaid tariff without her consent or participation.

Particulars of data breaches and data privacy infringement by BD T/A Bd East Africa and Safaricom

23. Both BD and Safaricom as data controllers and data processors by their acts or omissions initiated a security breach that affected the dignity, confidentiality, integrity and availability of the Complainant's personal data resulting in personal data breach.

24. BD and Safaricom violated the Complainant's fundamental human right to dignity and privacy under Art. 19, 28 and 31 of the Constitution through the processing of the Complainant's personal data contrary to the laid-out laws and regulations.

25. BD and Safaricom violated the Complainant's consumer protection rights guaranteed under Art. 46 of the Constitution to services of reasonable quality from BD and Safaricom; information that is necessary for the Complainant to

gain full benefit from the service; protection of their safety and economic interest; compensation for their loss as a result of data breach.

26. The 1st Respondent failed in processing the Complainant's personal data in a lawful, fair and transparent manner by failing to:

    i. Explicitly specify the legitimate purpose for which the personal data was being collected during the pre-employment phase contrary to section 25 (b) of the Data Protection Act.
    ii. Processing the Complainant's personal data in a manner incompatible with the purposes for which the personal data was collected during the pre-employment application process (for verifying the accuracy of the Complainant's details, supporting and fulfilling the employment contract as a HR requirement) contrary to section 25 (c) of the Data Protection Act.
    iii. Collecting the Complainant's personal data without providing a valid explanation where the Complainant's information related to family affairs contrary to Section 25 (e) of the Data Protection Act and the Consumer Protection Rights under Art. 46.
    iv. To obtain consent from the Complainant even after her contract with BD had been terminated.
    v. Cross-border transfer of the Complainant's personal data outside Kenya without proof of adequate data protection safeguards or consent from the Complainant in contravention with Section 25 (h) of the Data Protection Act, 2019.
    vi. Failure to disclose to the complainant the relevance of her personal data to the purposes for which it is to be used during the pre-employment application phase contrary to Data Protection Act.

Particulars of breach of Kenya Information and Communications (Registration of Sim-Cards Regulations) by the tele-communication operator (Safaricom)

27. The Complainant alleges that Safaricom failed to abide by regulation 6 and 7 of the Kenya Information and Communications (Registration of SIM-Cards Regulations).
28. Further, that Safaricom failed to verify the Complainant's information as required by law and failure to require the production of the original identification card from the Complainant.
29. Failure by Safaricom to present the Complainant with any forms to fill nor sign any SIM Card registration forms/transfer of ownership forms as required by the law.
30. Failure by Safaricom to require the Complainant to appear in person and issue her consent during the transfer/registration of the transferred BD billed number to the Complainant's Identity card under the Safaricom's prepaid tariff.
31. The transfer and registration of the Complainant's private SIM card /number by the former employer (BD) on the Complainant's behalf without her consent was not stated as the intended purpose of collecting her national Identification particulars during the pre-employment application process. It is thus unlawful and ultra-vires.

Particulars of data breaches under the global policy by BD T/A BD East Africa

32. The Complainant alleges that the 1st Respondent failed to abide by its commitment to good stewardship of all Personal Data of its products, its internal systems and its day-to-day work and further failed to carry out its business activities in compliance with applicable international and national data protection laws.
33. Failure to make available to individuals from whom, or about whom, personal data is collected, information about its policies and practices relating to the processing of personal data, including what data is collected, how it will be processed (including to whom it may be disclosed and/or transferred) and contact information for submitting inquiries or complaints and any rights or choices available to individuals in connection with the Personal Data under the control of BD.

34. Failure to offer choices to the Complainant regarding collection and processing of her personal data and make such choices readily available to the Complainant and follow the choices and controls that BD must make available to the Complainant.
35. Failure to minimize collection of the Complainant's personal data by its agent to the extent that it is reasonably necessary and related to the purposes for which the Personal Data is obtained.
36. Failure to retain the Complainant's personal data as long as needed for those purposes for which it was required.
37. Failure to limit processing of the Complainant's Personal Data to uses reasonably expected by the Complainant in which the Personal Data was collected-verification of the accuracy of the Complainants' details, supporting and fulfilling the employment contract as a HR requirement during the pre-employment application process.
38. Failure by the Information Security Risk Council (ISRC), Chief Privacy Officer (CPO), Chief Information Security Officer (CISO), Data Protection Officer (DPO), Director Product Security/Product Security Officers, National Data Protection Coordinators (NDPCs), and business or technology owners of IT Systems to manage the data breach and take steps to prevent further harm within 72 hours of its occurrence.
39. As a result, the Complainant makes the finding that there were violations of the Right to dignity and privacy guaranteed under Art. 19, 28 and 31 of the Constitution. Further, that the Respondents BD and Safaricom violated the Complainants right to dignity and privacy by:
    i. Collecting the Complainant's personal details during the pre-employment application phase, using, storing, sharing and disclosing of the Complainant's personal data without her consent.
    ii. Further the Respondent BD initiated cross-border transfer of the Complainant's personal data outside Kenya without proof of adequate data protection safeguards or consent from the Complainant.
    iii. BD through its agent gave instructions and authorized Safaricom to carry out registrations of the Complainant's private mobile number/SIM card, provided copies and details of her national ID card, and together with Safaricom, BD went to the extent of deciding the choice of tariff

the Complainant should be put on for her private/personal SIM card without her prior informed consent.

iv. The Complainant avers that the role of BD as a data processor should have ended upon termination of any agreement that BD had with Safaricom regarding her corporate line.

v. The Complainant further avers that even in cases where there is the option of online registration without having to visit the telecommunication operator store, the data subject who is the National Identity Card owner would be required to fill out the registration details on their own and upload their own identification documents for registration and verification/self-attesting.

vi. It is the Complainants submissions that the processing of any details regarding the Complainant's private mobile number/SIM card registration, sharing of national ID copies/details and subsequent choice of tariff should have been handled by the Complainant who is the identity card holder or intended subscriber. That copying the Complainant in some of the email communications between BD former employer and Safaricom that the Complainant saw weeks later in her private email inbox does not amount to giving consent for her personal/sensitive data to be processed through an unlawful SIM card registration process.

vii. The Complainant further submits that the unauthorised handling and sharing of her personal/sensitive data by her former employer (BD) was unnecessary, careless, and with NO legitimate purpose or legal basis. After the deactivation of the BD billed SIM card, the Complainant's former employer (BD) needed to ensure the deactivation of the corporate billed SIM card and perhaps inform Safaricom that the Complainant would be the new subscriber to whom the line was being transferred to while adhering to all the requirements under the Kenya Information and Communications Act; actions which do not require disclosure of the Complainant's National Identity Card copies containing personal/sensitive data.

viii. That it is upon the Complainant to decide if, how, when, where and on what tariff she wanted to register her personal SIM card. On 4/10/2024 B**** O****** emailed M**** M*****confirming that the transfer of the terminated BD billed mobile number to the Complainant's National Identity Card had been completed.

40. The Complainant further alleges the violations of the Consumer Protection Rights guaranteed under Art. 46 of the Constitution:

i. The Respondents BD and Safaricom have violated the rights of the Complainant to protection of their health, safety, and economic interests by misuse and unlawful handling of the Complainants personal information through the act of unauthorized and unlawful registration of her private SIM card which put the Complainant at risk of exposure of her sensitive and personal information about her date of birth , biometric data, citizenship, all her three names, gender, place of birth, her national Identity serial number, other biographic data, National ID card photo, as contained in the national identity card to third parties including cross-border transfer of her personal data without her authorization.

ii. BD contravened the Complainant's consumer protection rights by not ensuring the services are of reasonable quality in the context of establishing Data Processing Agreements with Safaricom stipulating how personal data may be used to fulfil the purpose of the commercial agreement.

iii. BD and Safaricom contravened the Consumer Protection Rights by failing to ensure redress mechanisms are in place that manage data breach and take steps to prevent further harm within 72 hours of its occurrence. Further, to Compensate loss or injury arising from defects of services offered in the context of data protection.

Particulars of loss and damage

41. As a result of this occurrence and the numerous violations:

i. The Complainant has suffered loss of control over her data and her right to privacy and dignity has been grossly violated through the

irresponsible, irregular and unlawful actions of her former employer (BD) and Safaricom PLC.

ii. Complainant has suffered health, safety, and economic violations by misuse and unlawful handling of her personal information through the act of unauthorized and unlawful registration of her private SIM card which put the Complainant at risk of exposure of her sensitive and personal information about her date of birth , biometric data , citizenship, all her three names, gender, place of birth, her national Identity serial number, other biographic data, National ID card photo, as contained in the national identity card to third parties including cross-border transfer of her personal data without her authorization.

iii. The Complainant has been subjected to significant emotional distress and anxiety. She has been unnecessarily exposed to the risk of identity theft, impersonation, risk of financial loss as her personal mobile number, Identification card copies containing personal data coupled with her personal email address have been unnecessarily shared with third parties including across borders to unauthorized individuals.

42. The Complainant has also incurred a direct cost as a result of pursuing redress and compensation for the violations she has suffered. The Complainant has had to secure the services of a lawyer to document and represent her in the adjudication process. An action which has costed the Complainant Kshs. 200,000.

43. The Complainant adduced the following documents as evidence:

i. Global policy.
ii. A copy of the employment contract.
iii. Copies of the email correspondence dated 3rd August 2021.
iv. A copy of the National Identity Card.
v. A copy of the email correspondence dated 3rd October 2024
vi. Certificate of Service.
vii. A copy of the termination letter.
viii. A copy of the clearance form.
ix. A copy of the Advocates invoice.

44. The Complainant prays for the following reliefs:

a) A declaration that the Respondent BD and Safaricom by collecting, structuring, organizing, using, storing, sharing and disclosing of the Complainant's personal data without her consent is unconstitutional and a violation of the Complainant's enjoyment of fundamental rights under Art. 19, 28 and 31 of the Constitution and Data Protection Act.

b) A declaration that BD and Safaricom violated Art. 46 of the Constitution by processing of any details regarding the Complainant's private mobile number/SIM card registration, sharing of national ID copies and details and subsequent choice of tariff for the Complainant without her consent or participation;

c) A declaration that Safaricom violated regulation 6 and 7 of the Kenya Information and Communications (Registration of SIM-Cards Regulations) by failing to verify from the Complainant the SIM Card transfer and registration information provided as required by law; failing to require the Complainant to appear in person and produce the original identification card; failure to present the Complainant with any forms to fill nor sign any SIM Card registration forms as required by the law.

d) A permanent injunction do issue restraining the Respondents BD and Safaricom jointly and severally either acting on their own and or through its agents, employees, servants, and/or any other person acting and/or purporting to act under their instructions or orders from further accessing, collecting, structuring, organizing, using, storing, sharing and disclosing of the Complainant's personal data without her informed consent.

e) The Court do find that the Complainant is entitled to both general and exemplary damages for violation of her constitutional rights as enumerated above.

f) Special damages of Kshs. 200,000

g) Costs of the Claim and interest in e,f and g.

II. 1ST RESPONDENT'S RESPONSE

45. The 1st Respondent submitted a response to the notification of complaint in a letter dated 13th January, 2025 and further made an amended and tracked response dated 3rd February 2025.

46. In the response, the 1st Respondent alleges on or around 28 September 2021, the Company the Complainant entered into an employment agreement effective 16th August 2021, where the Complainant was employed as the Global Health Leader for Africa.

47. Prior to the start date, the Company shared all relevant material, including the Employee Privacy Notice with the Complainant, informing her of the Company's data processing policies and procedures including the kind of personal data the Company collects and the purposes it is used for. Furthermore, the Complainant underwent a training on the Company's staff handbook, where she was informed of all the Company's policies and where to find them.

48. The Complainant later signed a copy of the staff handbook acknowledging that she had read and understood everything in the handbook, including where to find all the Company's policies. Consequently, the Company, through one of its representatives, asked the Complainant for information, which included copies of the Complainant's national identity card, passport, Kenya Revenue Authority Personal Identification Number (KRA PIN) certificate, banking details, NSSF number and NHIF number.

49. After sharing the information with the Company, the Complainant was successfully onboarded and started her tenure of employment with the Company. Further, it is the Company's policy to provide eligible employees with mobile phones and mobile SIM cards for them to carry out their duties more efficiently for the Company, and this is strictly done in accordance with the Company's Mobile Phone Policy.

50. Pursuant to this Policy, the Complainant was to be provided with an official mobile telephone line for work purposes in one of two ways, that is, either by way of: a SIM card procured by the Company on behalf of the Complainant or a transfer of the Complainant's personal line to the Company's account with its

telecommunication service provider, Safaricom. Upon being offered these two options in an in-person meeting, the Complainant chose the latter option and opted to keep her personal mobile telephone line and number (+25473*******) (which was operated by Airtel at the time) and to have that telephone line transferred to the Company's account with its telecommunication service provider, Safaricom.

51. Further, to effect this transfer, the Complainant also signed a Number Porting Request Form dated 16 August 2021. The Complainant was also kept in copy in all emails regarding the mobile line transfer.

52. On 30th September 2024, the Complainant's employment contract was terminated. As part of her offboarding process, the Company required her SIM card to be taken off the Company's account with Safaricom. In order to facilitate the transfer of the Complainant's telephone number back to her on 3rd October 2024 at 0839hrs, the Company, through one of its representatives shared the Complainant's name and national identification card number with a representative from Safaricom, notifying them that the Complainant was no longer an employee of the company, and as such, they should help in transferring the line, including the accumulated Bonga points, from the company's account to the Complainant's personal account.

53. Further, on the same date, at 0913hrs, a representative from Safaricom confirmed that the line had been terminated from the Company's account, and for transfer to the Complainant's personal account to be affected, the Company would need to share a copy of the Complainant's Identity Card (ID). Still on the same date, at 0955hrs, the Company then shared a copy of the Complainant's Identity Card with Safaricom and the mobile line was consequently transferred to the Complainant on the next day, 4 October 2024, as confirmed by an email sent by Safaricom's representative to the Company's representative affirming the same.

54. Against this factual background, the 1st Respondent wishes to respond to the Complaint Notice and more particularly to the allegations therein which may be summarized as follows:

a. Response to Allegation 1 - that the 1st Respondent *allegedly failed to specify the purpose(s) for which the Complainant's personal data was being processed during the pre-employment phase*

55. In response to this allegation, the 1st Respondent denies that it failed to specify the purposes for which the Complainant's personal data was being processed during the pre-employment phase. The Company has an Employee Privacy Notice which all employees, including the Complainant, were informed about and asked to review before their employment.

56. As indicated under the 'For what purposes do we use your personal data, and why is it justified?' clause of the Company's Employee Privacy Notice, the Company clearly spells out the specific and legitimate purposes for which it processes personal data, some of which include: staff administration, such as managing work activities and personnel generally, including hiring and onboarding of employees; maintaining business operations, such as operating and managing technology and communication systems; emergencies and communications, such as facilitating communication between employees within the BD Group and/or with third parties as is necessary for business purposes and global initiatives; ensuring compliance, such as complying with BD policies and with local requirements, such as income tax and national insurance deductions; and health risk appraisals, which are only conducted as permitted and/or required by local law for the sole purpose of managing the employment relationship.

57. Furthermore, the Complainant underwent a training on the Company's staff handbook, where she was informed of all the Company's policies and where to find them. She later signed a copy of the staff handbook acknowledging that she had read and understood everything in the handbook, including where to find all the Company's policies. Therefore, by informing the Complainant about the Employee Privacy Notice (and all other Company policies), and asking her to review them before beginning her employment, the Company complied with the duty to notify contained under Section 29 of the Data Protection Act.

58. The Company therefore states that the above allegation is false, since the Complainant was informed about the Employee Privacy Notice and the purposes her personal data would be processed.

b. Response to Allegation 2 - that the Company allegedly processed personal data in a manner that is incompatible with the purposes for which the personal data was collected during the pre-employment application process

59. In response to the above allegation, the Company observes that the Complainant has not specified how the Company processed her personal data in a manner that is incompatible with the purposes for which it was collected or any purposes for which the Company allegedly processed her personal data that were incompatible with the original purposes for which such personal data was collected.

60. Furthermore, the Company also observes that the above allegation is contradictory to the allegations made in Allegation 1, where the Complainant alleges that the Company failed to specify to her the purpose(s) for which her personal data was being collected during the pre-employment phase. The question that begs to be answered is how was she able to make an assessment and arrive at the conclusion that there was an incompatibility of purposes if the said purposes had not been communicated to her. The Company denies the above allegation and states that it only processed the Complainant's personal data for the specific purposes set out in the Employee Privacy Notice.

61. These included, among others, the onboarding of the Complainant as an employee, providing her with necessary work-related facilities/benefits (such as mobile phone services on the Company's account) and compliance with regulatory requirements (that is, NHIF & NSSF statutory deductions as well as income tax remittances). The Company therefore states that all the personal data collected from the Complainant was used strictly for the purposes set out in the Company's Employee Privacy Notice.

c. Response to Allegation 3 - that the Company allegedly failed to provide a valid explanation for the processing of the Complainant's personal data relating to their private or family affairs contrary to Section 25(e) of the Data Protection Act

62. The Company states that the above allegation is false. The Company is cognizant of the requirement contained in section 25(e) of the Act to provide a valid explanation to the data subject where personal data relating to the subject's family

or private affairs is collected. In strict adherence to the same, the Company's Employee Privacy Notice, explains that the Company collects personal data including personal data of family members and defendants for the purpose of administering and providing benefits and other-work related allowances to the Complainant and her family. This explanation is contained under the 'For what purposes do we use your personal data, and why is it justified?' – Staff administration clause under the Employee Privacy Notice. The Company therefore reiterates that the above allegation is false and misleading, since a valid explanation was provided in the Employee Privacy Notice on why the Complainant's personal data relating to her family and private affairs was processed.

d. Response to Allegation 4 – that the Company allegedly failed to obtain consent for the transfer of the Complainant's line from the Company's account back to the Complainant after her contract with the Company had been terminated

63. As mentioned in the background above, it is the Company's policy to provide eligible employees with mobile phones and mobile SIM cards for them to carry out their employment duties, and this is strictly done in accordance with the Company's Mobile Phone Policy. Pursuant to the BD Mobile Phone: Appropriate Use clause, paragraph 3, the issuance of a SIM Card happens in one of two ways; one the Company procures the SIM card on behalf of the employee, or two an employee is given the option of transferring their personal line to the Company's account with Safaricom.

64. In the Complainant's case, she chose the latter and opted to keep her personal line, mobile number +25473*******, and to have the same transferred to the Company's account with Safaricom (please refer to the previously enclosed Number Porting Request Form and Email correspondence between the Company's Representative and Safaricom with the subject line 'New Entrant Activation – Catherine Murithi').

65. On 30 September 2024, the Complainant's employment was terminated by the Company on account of redundancy. As part of her offboarding process, the Company required her SIM card to be taken off its corporate account with

Safaricom since she was no longer an employee of the Company, and thus, was no longer entitled to employee benefits. To that effect, on 3rd October 2024, the Company through one of its representatives, shared the Complainant's name and national identification card number with a representative from Safaricom, informing them that the complainant was no longer an employee of the company, and as such, they should help in transferring the line, including the accumulated Bonga points, from the company's account to the complainant's personal account.

66. Further, on the same date, a representative from Safaricom (on the same email thread) confirmed that the line had been terminated from the Company's account, and for transfer to the complainant's personal account to be effected, the Company would need to share copies of the complainant's Identity Card (ID). Still on the same date, at 0955hrs, the Company, through its representative, shared a copy of the Complainant's Identity Card with Safaricom. The mobile line was then transferred to the complainant on 4th October 2024, as confirmed by an email dated the same day, sent by Safaricom's representative to the Company's representative affirming the same

67. Therefore, the Company, in processing the complainant's personal data in the manner described above, relied on the ground of necessity for legitimate interests provided for under section 30 (1) (b) (vii) of the Act. The sharing of the complainant's personal data (copy of national identity card) with Safaricom at that point was a necessary pre-requisite for the transfer of the Complainant's mobile line back to the Complainant.

68. In reliance on the ground of necessity for legitimate interest under section 30 (1) (b) (vii) of the Act, the Company processed the Complainant's personal data with a view to facilitating the retransfer of her mobile line to her as the mobile line originally belonged to the Complainant who through her continued use thereof during her employment had accumulated Safaricom Bonga points which the Company saw fit to transfer back to her. The Company did this to protect itself from any future lawsuits regarding any owed benefits (e.g. Bonga Points) that had accrued to the Complainant through her use of her line;

69. Further, this approach was necessary to achieve proper off-boarding of the Complainant from the Company and no harm or prejudice was caused to the Complainant's rights and freedoms, as the mobile line was originally hers and Safaricom already had her personal data (copy of her national identity card) the same having been shared with Safaricom with the Complainant's knowledge and approval when the Complainant was first employed with the Company.

70. In providing her national identity card to Safaricom at the end of the Complainant's employment, the Company merely sought to restore full ownership and control of the Complainant's mobile line to her and to ensure that it did not continue providing an employment benefit to a non-employee. Therefore, the Company states that it lawfully processed the Complainant's personal data at the point of the termination of her employment as part of its routine employee offboarding procedures and on the basis of necessity for legitimate interests as provided for under section 30(1) (b) (vii).

e. Response to Allegation 5 - that the Company allegedly transferred the Complainant's personal data outside of Kenya without proof of data protection safeguards or consent from the Complainant

71. As mentioned above in response to allegation 4, after the Complainant's termination of employment, the Company requested Safaricom to transfer the Complainant's mobile line from the Company's account to the Complainant herself. Safaricom then requested for copies of the Complainant's identification document which were shared with Safaricom, through their representative.

72. The Complainant also alleges that the Company transferred her personal data outside of Kenya without her consent or proof of data protection safeguards. She alleges that such transfer of her personal data was effected through the copying in of two South African based colleagues to the Company's email to Safaricom dated 3rd October 2024. Pursuant to Section 25 (h) of the Act and Regulation 40 of the Data Protection (General) Regulations (the General Regulations), the transfer of personal data outside of Kenya is allowed where there are appropriate safeguards or consent from the data subject.

73. Furthermore, Regulation 41 of the General Regulations states that the requirement for appropriate safeguards is met where there is a legal instrument containing appropriate safeguards equivalent to the Act or where the data controller has assessed all the circumstances surrounding the transfer and concluded there are appropriate safeguards. In this respect, the requirements of the Act and the General Regulations, have both been met by the Company. Regulation (41) (a) of the General Regulations has been met in so far as the transfer of the Complainant's personal data, specifically, her National Identity Card Number, was made to South Africa which has enacted the Protection of Personal Information Act which can be said to be equivalent to the Act.

74. Regulation 41 (1) (b) of the General Regulations is satisfied as the employees of Becton Dickinson South Africa are subject to employment contracts which include confidentiality clauses that prevent the disclosure of the Complainant's personal data (please find attached the employment contracts - with confidentiality clauses - that the South African based employees were subject to).

75. Moreso, the concerned employees are also subject to the BD's Employee Privacy Notice (enclosed) which requires organizational safeguards such as the training of employees on how to handle personal data. Therefore, the Complainant's personal data was transferred outside of Kenya with appropriate safeguards in place.

76. Further the transfer of the Complainant's personal data to South Africa by copying in two of the South Africa based colleagues in the email to Safaricom was necessary because they were part of the Local Finance team in Kenya, even though they were based in South Africa. Their involvement was crucial for financial matters related to the Kenyan office, and that is why they were copied in the email in the first place.

f. Response to Allegation 6 – that the Company allegedly failed to report an alleged data breach to the ODPC within seventy-two hours

77. The Company denies that there was a personal data breach within the meaning of Section 2 of the Act. The said section 2 defines a personal data breach as a breach of security that results in the accidental or unlawful processing of personal data. As per the narration of facts in the Complaint Notice, the Complainant has not

demonstrated any factual circumstances that resulted in any accidental or unlawful processing of personal data yielding a personal data breach.

78. The 1st Respondent maintains that the processing of personal data by the Company was lawfully based on necessity for the legitimate interests pursued by the data controller and did not prejudice the rights and freedoms or legitimate interests of the Complainant. As such, we assert that no personal data breach occurred and none has been shown by the Complainant to have occurred. The Complainant further alleges that the failure to report a breach is a violation of its constitutional rights under Article 46 of the Constitution of Kenya which protects consumer rights. However, such a claim is outside of the jurisdiction of the ODPC as Section 8 (1) (f) of the Act limits the ODPC's jurisdiction to infringements under the Act.

79. Consumer protection issues are outside the scope of the ODPC's jurisdiction and should be litigated before alternative forums. Further, since no personal data breach occurred in this case, no corresponding data breach reporting or notification obligation can rightly be said to have arisen.

g. Response to Allegation 7 – that Safaricom failed to comply with the requirements of the Kenya Information and Communications (Registration of SIM-Cards) Regulations (Registration of SIMCards Regulations)

80. The Complainant alleges in their Complaint that Safaricom failed to comply with the requirements of the Kenya Information and Communications (Registration of SIM-Cards) Regulations. As stated above, Section 8 (1) (f) of the Act states that the ODPC can only determine complaints on the basis of infringements under the Act. Therefore, any claims premised under the Kenya Information and Communications Act or any regulations under it cannot properly lie before the ODPC for determination.

h. Response 8 – the Complainant is not entitled to the reliefs sought In the Complaint Notice, the Complainant has requested for the following remedies to be issued by ODPC:

81. As enumerated above, issues pertaining to the interpretation of the Constitution and the application of Registration of SIM-Cards Regulations are outside the jurisdiction of the ODPC and fail on that account. Therefore, the reliefs sought under point 1 and 3 above are unwarranted. Moreso, Regulation 14 (3) of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations (the Enforcement Regulations) only provide for the following remedies: (a) issuance of an enforcement notice to the respondent in accordance with the Act and these Regulations; (b) issuance of a penalty notice imposing an administrative fine where a respondent fails to comply with the enforcement notice; (c) dismissal of the complaint where it lacks merit; (d) recommendation for prosecution; or (e) an order for compensation to the data subject by the respondent. The Enforcement Regulations do not provide for the issuance of a permanent injunction to prohibit the processing of a data subject's personal data.

82. Nonetheless, the Company wishes to assert that the further processing of the Complainant's personal data is required by various laws including Section 74 of the Employment Act and Section 23 of the Tax Procedures Act. Therefore, the continued processing of the Complainant's is required for compliance with legal obligations to which the Company is subject, falling within the basis of lawful processing under Section 30 (b) (ii) of the Act. This renders an injunction preventing further processing impracticable. Therefore, as per our responses to the allegations above, we do not believe that the Complainant is entitled to any of the reliefs sought.

83. The 1st Respondent adduced the following documents as evidence:

i. Letter of notification of complaint dated 12 December 2024 which is addressed to Becton Dickinson and Company t/a BD East Africa (Annex 1).
ii. Number Porting Request Form dated 16 August 2021 (Annex 2).
iii. Email correspondence between the Company Representative and Safaricom with the subject line 'New Entrant Activation – Catherine Murithi' (Annex 3).

iv. Employee Privacy Notice – EMEA Region last revised 2 October 2023 (Annex 4).

v. Signed copy of the staff handbook signed by the Complainant on 22 Aug 2021 (Annex 5).

vi. BD East Africa Mobile Phone Policy dated 1 February 2021 (Annex 6). Email correspondence between the Company's Representative and Safaricom with the subject line 'Exit Notice – Catherine Murithi - +254 735182202' (Annex 7).

vii. Two (2) Employment Contracts – with the confidentiality clauses - of the South African based employees (Annex 8 & 9).

II. 2ND RESPONDENT'S RESPONSE

84. The 2nd Respondent asserts that it is clear from the particulars of the complaint that the Complainant was in an employment relationship with Beckton Dickinson & Company t/a BD East Africa ("the First Respondent"). Further, the 2nd Respondent was not privy to the circumstances of the employment relationship between the Complainant and 1st Respondent, save for the much that has been admitted by the Complainant, which explains the genesis of the customer relationship between Safaricom and the Complainant.

85. Safaricom acted on the instructions of the 1st Respondent to have the Complainant's mobile number 0735****** billing information aligned to her employer's details to enable payment of her phone bills during the tenure of her employment. This followed the Complainant having authorized her employer to process her number and ID details for this purpose.

86. The 1st Respondent similarly notified Safaricom on 3rd October 2024 that the Complainant had exited employment and for the phone number to be transferred back to her for billing purposes. Bonga points acquired during her employment were also moved to her personal account as these are her property to deal with as she wishes.

87. Safaricom facilitated the 1st Respondent's request after having verified the Complainant's ID documentation. The Complainant was now free to use the phone number with no limitations.

88. In the circumstances, the 2nd Respondent deems the current complaint as against Safaricom premature as the Complainant has not engaged them for regularization of her details to her satisfaction. Any previous registrations and terminations were done on the basis of performance of her employment contract. However, the 2nd Respondent does not agree with the position that processing her personal data to offer her communication services at her employer's cost contravened any laws or regulations.

89. The 2nd Respondent therefore maintains that the complaint against Safaricom should be dismissed and further reiterates Safaricom's commitment to its obligations to protect the personal information of data subjects.

III. COMPLAINANT'S RESPONSE TO THE 1ST AND 2ND RESPONDENTS' RESPONSE

a. Rejoinder to the 1st Respondent

90. The Complainant categorically states that the purported allegation that prior to the start date 16/08/2024 (the day she reported to work as a new employee), BD shared 'all relevant materials" including an "Employee Privacy Notice", and informed the Complainant of BD's data processing policies and procedures including the kind of personal data the company collects and the purposes for which it is used are falsehood as she did not receive any documents or institutional policies and/or informed of why her personal data was being collected. The obligation to produce evidence of receipt of such documents rests on BD.

91. As indicated in the Complainant's statement dated 27th November 2024, she only received communication via email on 3rd August 2021 from the Office Administrator asking her to share her personal and sensitive documents. When Administrator asked the Complainant for the personal information on 3rd August 2021 there was no contract in place and the Complainant's start date was 16th August 2021, the date which the employment contract became effective.

92. The Complainant reiterates that neither was the purpose of collecting her personal and sensitive data nor her rights were communicated and puts BD to strict proof. Further the privacy notice shared by the 1st respondent(BD) which was last revised

on 2nd October 2023 is an incomplete document as it is not signed and lacks the revision log, approvers and authorizers as demonstrated in the Global Policy Shared by the Complainant in the complaint dated 27th November 2024; a clear indication of a document that is still under development and has not been approved and disseminated to employees. This explains why it was never shared or accessed by the Complainant prior to porting her line and prior to the pre-employment phase and could not be accessed at the HR one portal or displayed in public spaces during her employment tenure.

93. The Complainant denies having gone through any form of training on the company's staff handbook. She however confirms that days after joining BD on 22/08/2021, she was given a soft copy of the handbook which she read and executed. She further states that she familiarized herself with BD policies which were available in HR one portal but did not come across any purported "Employee Privacy Notice" or Mobile Phone Policy and neither did she sign any privacy notice or Mobile phone policy.

94. It is also noteworthy that the handbook was accessed on 22nd August 2021 after the porting and transfer of the Complainant's private mobile number/SIM card to BD account and sharing of the Complainants national ID copies. The handbook also does not have specifications on the use to which personal data collected shall be made use of, particularly the Complainant's ID.

95. Further to the alleged trainings which were never undertaken by BD, all relevant online internal training on standard operating procedures (SOP), policies, manuals during the Complainant's employment tenure happened on the BD platform called C2C where upon completion, the employee would be issued with a certificate of completion. Therefore, it is expected that the alleged trainings that BD is purporting to have undertaken should be supported with an authentic certificate of completion to prove that this training actually took place. A training on the handbook should have automatically generated a certificate of completion confirming participation. Such evidence has not been adduced before this adjudication body and I would seek orders of production of the certificate of

completion for this handbook training that BD purports that the complainant undertook.

96. The Complainant further states that BD was in violation of the provisions of Section 29 of the handbook provides that notices are to be displayed at 'various places' including the Intranet.BD did not display the Privacy Notice in any place including the intranet where the Complainant could access it.

97. The Complainant agrees with the 1st Respondent to the extent that she was asked for her private and sensitive data through BD's representative. However, the request for her private and sensitive information was inquired into before going through the handbook on 22/08/2021. BD through their representative asked for a set of the Complainant's personal and sensitive data in the form of copies of documents as well as forms where she was required to input her personal data on the 03/08/2021, thirteen days before joining BD. The said documents were shared with representative on 05/08/2021. These documents comprised of birth certificates of the Complainant's children, copies of ID, copy of the Complainant's passport, KRA PIN, NSSF, NHIF, Proof of banking, drivers' license, passport size photos of the Complainant's children.

98. It is worth noting that the Complainant shared her ID Copies on 5th August 2021 after which BD shared her ID copies with Safaricom to facilitate the unlawful transfer of 073******* from the Complainant to BD by the 18/08/2021. A look at the evidence furnished by BD titled Number Porting Request Form under the sub-theme For Official Use Only, is clear that the verification of the subscriber's identification in order to obtain her consent and original documents by Safaricom was never done.

99. The transfer of the Complainant's data by BD to Safaricom was also effected before the Complainant being informed of and accessing the handbook on 22/08/2021 or the purported Privacy Notice. This clearly demonstrates that BD is approaching this adjudicating body with unclean hands tainted by inconsistencies, falsehood and misrepresentation.

100. The Complainant alleges that she never accessed the Mobile Phone Policy in the HR one portal. Also, the sharing of her ID to Safaricom, porting and transferring

of her Airtel line 073******* took place on 16th of August to 18th August 2021 before accessing the handbook and any policies. As particularized in her Complaint dated 27th November 2024, the Complainant was asked by 1st Respondent's representative via a telephone conversation to Port her line from Airtel to Safaricom and subsequently completed the porting forms – authorizing the porting of 073******* from (Airtel)to (Safaricom).

101. It should be noted that the Complainant never at any one point consented to her ID number/copies being shared to Safaricom by BD or used to transfer ownership of the same number to BD. Neither did she consent to having BD use her ID details to transfer the same line after conclusion of her employment contract with BD.

102. The Complainant further states that she was never advised of the option of being provided with BD procured mobile SIM cards by the company but was instead offered the option of porting and transferring her personal Airtel line 0735****** to Safaricom and was issued with the porting form to sign. However, as indicated above the Porting Request Form under the sub-theme For Official Use Only, it is clear that the verification of the subscriber's identification during porting and transfer in order to obtain her consent and original documents was never done by Safaricom.

103. The mobile phone policy dated 1st February 2021 was never availed to the Complainant and is unsigned in the employee signature section clearly depicting the inconsistencies, falsehood and misrepresentation.

104. Whereas the mobile phone policy shared by the respondent (BD) provides for the issuance and usage of the company's owned mobile telephones, it does not make provision for use of the employee's personal data by BD to port and transfer the employees' line to BD billing account before or after termination. As particularized in the complaint dated 27th November 2024 and supported by the company's clearance sheet the required action during clearance was deactivation of the BD SIM card and not transfer of ownership.

105. The Complainant further contends that BD is not registered as a data controller or data processor in accordance with the Data Protection (Registration of Data

Controllers and Data Processors) Regulations therefore grossly violates the laws of Kenya when in control and procession of personal data of persons including the Complainant without complying with the Kenyan legal and policy framework. As such, they have demonstrated that they do not have sufficient internal safeguards to guarantee protection of data.

106. Section 40(1)(b) provides that a data subject may request a data controller or data processor to erase or destroy without undue delay personal data that the data controller or processor is no longer authorized to retain. They Complainant submits that the Respondents ought to be compelled by this Office to seize storing the Complainant's personal data. If possible, an order do issue directing BD to delete the Complainant's personal data permanently and share proof of having done so.

107. The Complainant reiterates that the processing of her data post-employment and cross-border transfer without her consent under the cover of a purported unconstitutional privacy notice that apply to former employees has violated her Constitutional right to privacy, property and consumer protection that warrants this adjudicating body to grant a permanent injunction to stop any further processing of her data.

108. The Complainant confirms that BD admits having shared her name and national ID number with third parties without her consent.

109. With regards to the allegation 1: The Company failed to specify the purpose for which the Complainants personal data was being collected during the pre-employment phase. The Complainant vehemently asserts that she was never informed about ', "employee privacy notice" and neither was she able to access it in the HR one portal nor did she go through any form of training with respect.

110. On allegation 2: The Company processed the Complainant's personal data in a manner incompatible with the purposes for which the personal data was collected during the pre-employment application process, BD's Office Administrator did not inform the Complainant of the use to which her personal data was to be put, the legitimate expectation was that the personal data was relevant for the purposes of verifying the accuracy of the Complainant's details, supporting and fulfilling the employment contract as a HR requirement during the pre-employment application

process. In addition, the Complainant had a legitimate expectation that BD would not disclose her personal information to third parties without consent.

111. On allegation 3: that the company failed to provide a valid explanation for the processing of the Complainant's personal data related to family affairs. The Complainants challenges the Respondent to demonstrate that her averments are false and submits that she is a stranger to the Employee Privacy Notice and has never seen or been trained on any such policy. Further, the privacy notice in shared by the respondent which was last revised on 2nd October 2023 is an incomplete document as it is not signed and lacks the revision log, approvers and authorisers as demonstrated in the Global Policy shared by the Complainant in her claim dated 27th November 2024.

112. On allegation 4: the company failed to obtain consent for the transfer of the Complainant's line from the company's account back to the complainant after her contract with BD had been terminated. The Complainant states that the mobile phone policy dated 1st February 2021 was never availed to the Complainant and is unsigned in the employee signature section clearly depicting the inconsistencies, falsehood and misrepresentation being presented before the data commissioner.

113. On allegation 5: The Company transferred the Complainant's personal data outside Kenya without proof of adequate data protection safeguards or consent from the Complainant. The Complainant asserts that the 1st Respondent has failed to demonstrate the effectiveness of the security safeguards put in place internally by BD as well as the recipient country. Further, BD has violated the Data Protection Regulations by failing to ascertain before transferring the Complainant's data out of Kenya that there are appropriate data protection safeguards internally and in the recipient, country thus exposing the Complainant to identity theft and misuse of her personal data.

114. On allegation 6: The Company failed to report the data breach to ODPC within 72 hours. The Complainant disassociates with the contents of allegation 6 and vehemently reiterates that the processing of her personal information including cross-border transfer is unfair, unlawfully, prejudicial, a threat to personal safety and infringement to her person's privacy. It is the Complainant's contention that

the gross infringement was evident following the disclosure of her ID and personal email address against her will.

115. On Allegation 7: Safaricom Failed to comply with the requirements of Kenya Information And Communications (Registration Of Sim-Cards Regulations). The Complainant disassociated with the contents of allegation 7 and posits two equity maxims:

i. He who seeks equity must do equity: If BD and Safaricom seek to be discharged from liability, they must demonstrate that they have acted fairly within the laws and regulations that have been prescribed to facilitate data security. This adjudicating body should not be made to belief that it does not have jurisdiction to place reliance on the Kenya Information And Communications (Registration Of Sim-Cards Regulations) which should be read together with the Data Protection Act and the Constitution for purposes of placing reliance and verifying whether the structures and procedures put in place to ensure data security and privacy are followed. Therefore, if BD and Safaricom seeks equity they must also demonstrate that they have done justice and equity.

ii. BD clearly faked the identity by playing the role of the Complainant in the transfer of her personal mobile number and went further to verify on the Complainant's behalf. It is noteworthy that Safaricom in their response dated 27th December 2024 mischievously confirms having verified the Complainant's identification.BD in its legitimate economic business interest falsified the Complainants personal information thus infringing regulation 6 and 7 relating to Kenya Information and Communications (Registration Of Sim-Cards Regulations) with respect to registration of existing and new subscribers of telecommunication services. This process guarantees the right to accuracy, right to privacy and control of personal data by the data subject and therefore cannot be excluded or isolated in matters data protection.

iii. He who comes to equity must come with clean hands: The Complainant posits that this principle requires that a person who seeks remedy demonstrates that he/she has not acted improperly or unconscionably. The principle requires

that an adjudicating body ceases to issues an equitably remedy to a person who has not acted equitably. By not acting in compliance with the Kenya Information And Communications (Registration Of Sim-Cards Regulations), in giving instructions and authorisation to Safaricom to carry out registrations of the Complainant's private mobile number/SIM card and provided copies and details of her national ID card, and together with Safaricom going to the extent of deciding the choice of tariff for the Complainant's private/personal SIM card without the Complainant's prior informed consent is a gross infringement of the Kenya Information And Communications (Registration Of SimCards Regulations) and prejudicial to her right to privacy. This is because the Complainant's prior informed consent was not obtained.

iv. It is worth noting that the Complainant shared her ID Copies on 5th August 2021 and BD shared her ID copies with Safaricom to facilitate the unlawful transfer of 073******* from the Complainant to BD by the 18/08/2021. A look at the evidence furnished by BD in Annexure 2 titled Number Porting Request Form under the sub-theme For Official Use Only, it is clear that the verification of the subscriber's identification in order to obtain her consent and original documents by Safaricom was never done. The transfer of the Complainant's data was also effected before being informed of and accessing the handbook on 22/08/2021 or the purported Privacy Notice. This clearly demonstrates that BD is approaching this adjudicating body with unclean hands tainted by inconsistencies, falsehood and misrepresentation. BD can therefore not mislead this adjudicating body to overlook the Kenya Information and Communications (Registration Of Sim-Cards Regulations) in its interpretation of what constitutes fair, lawful, accurate and transparent processing of data under the assertion that it lacks jurisdiction. It is our submission that the Kenya Information And Communications (Registration Of SIM-Cards Regulations) should assist this court in determining the structures and processes set in place to ensure the security of data.

116. The Complainant prays that:

i. The response to the notification of claim be dismissed and the claim against BD and Safaricom be allowed with costs as particularized in the Reliefs Sought in the Statement of Claim dated 27th November 2024

ii. BD and Safaricom be compelled to produce all the forms and documents containing the Complainant's personal information that they used for transfer of 073****** and the verification exercise as admitted by Safaricom in their response dated 27th December 2024.

iii. A production order do issue to BD with respect to certificates of completion of the purported training undertaken in relation to the handbook training, Employee Privacy Notice training and Mobile Phone Policy Training.

iv. An order do issue directing BD to delete the Complainant's personal data permanently and share proof of having done so.

b) Rejoinder to the 2nd Respondent's response

117. The Complainant agrees with the 2nd Respondent to the extent that Safaricom acted on the instructions of BD to have her post-paid personal Airtel number +25473****** registered with a new carrier; Safaricom under the BD account for billing purposes. She however denies having authorized her former employer to process her ID details for purposes of registration and transfer of number +25473****** both during and after termination of her contract.

118. The Complainant reiterates that she did not consent/authorize the use and processing of her national ID by BD and Safaricom for registration and transfer of number +25473******* both during and after termination of her contract.

119. The 2nd Respondent, Safaricom, claims to have acted on the basis of the employment contract between the Complainant and BD however, the Complainant states that her employment contract has no mention of how BD was to utilize her personal data including her ID. Therefore, Safaricom and BD should have sort consent from the Complainant knowing that they were processing her data outside the said employment contract.

120. It is also noteworthy that the illegal transfer of number +2547******** to the Complainant happened on 4th October 2024 after the termination of the Complainant's employment contract with BD. She further states that verification

exercise as provided for in Regulation 6 and 7 of the Kenya Information and Communications (Registration of SIM-Cards Regulations) requires the Complainant's to appear in person, produce original ID or other identification documents and fill in the requisite forms. She states that this was never done by Safaricom.

121. Contrary to claims by the 2nd Respondent, the Claim before this adjudicating body in relation to Safaricom is timely and ripe as it demonstrates Safaricom's failure to live by its commitment and obligations to protect the personal information of data subjects by:

a. Failing to abide by data protection laws and regulation 6 and 7 of the Kenya Information and Communications (Registration of SIM-Cards Regulations)

b. Failing to verify the information provided from the Complainant as required by law

c. Failing to require production of the original identification card from the Complainant.

d. Failing to present the Complainant with any forms to fill nor sign any SIM Card registration forms as required by the law.

e. Failing to require the Complainant to appear in person and issue her consent during the registration of the transferred BD billed number to the Complainant's Identity card under the Safaricom's Uwezo tariff.

IV. INVESTIGATIONS UNDERTAKEN

122. The Office examined the complaint lodged by the Complainant, including evidence adduced in support thereof, the Respondents' written response, and all documents submitted by both parties as evidence.

V. ISSUES FOR DETERMINATION

123. It is not in contention that the Complainant was a former employee of the 1st Respondent and that the Complainant's Airtel phone number was ported from Airtel to Safaricom in order for the same to be billed from the 1st

Respondent's corporate account with the 2nd Respondent from the evidence adduced. However, upon termination of her employment contract, the 1st Respondent terminated the said SIM card from its corporate account and further transferred the same to the Complainant by sharing a copy of her personal ID to the 2nd Respondent.

124. In light of the above, the following issues fall for determination by this Office:

i. Whether the Office has jurisdiction over the complaint.
ii. Whether there was unlawful processing of the Complainant's personal data.
iii. Whether the Respondent violated the Complainant's rights under the Act and attendant Regulations.
iv. Whether the Complainant is entitled to any remedies under the Act and the attendant Regulations.

I. WHETHER THE OFFICE HAS JURISDICTION OVER THE COMPLAINT

125. The Complainant particularized various violations under the Constitution of Kenya, 2010 as mentioned hereinbefore including Articles 19, 28, 31 and 46. Further, the Complainant requested the Office to make declarations for the violation of the said constitutional rights and fundamental freedoms. The Respondent however challenged the jurisdiction of this Office in dealing with Complaint with regard to the mentioned constitutional violations.

126. In that regard, the Office concludes that Regulation 14(3) of the Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021 provides for various remedies that does not involve making declarations of a violation of any constitutional rights and specifically the ones as requested by the Complainant as the same is a preserve of the High Court of Kenya. In that regard, the Office lacks jurisdiction to investigate and make a determination to that extent.

127. The Complainant also requested the Office to make a declaration that the 2nd Respondent violated Regulation 6 and 7 of the Kenya Information and Communications (Registration of SIM-Cards Regulations) by failing to verify from

the claimant the SIM Card transfer and registration information provided as required by law; failing to require the Claimant to appear in person and produce the original identification card; failure to present the Claimant with any forms to fill nor sign any SIM Card registration forms as required by the law. Similarly, the Office lacks the jurisdiction to make such a declaration as the same is not envisaged under the Data Protection Act,2019. However, the Office has the latitude to investigate the potential data protection issues that may arise therefrom in the performance of those functions.

128. To that extent, the Complainant has raised issues pertaining to the lack of consent and authorization of the use of her personal data by the Respondents in processing and transfer of the phone number +2547********* from the 1st Respondent's corporate account with the 2nd Respondent and further on the issue of the transfer of the said number back to the Complainant.

129. To that end, the Office finds that it has the jurisdiction to entertain the complaint herein due to the privacy issues espoused above.

II. WHETHER THERE WAS UNLAWFUL PROCESSING OF THE COMPLAINANT'S PERSONAL DATA

a. *Allegation 1- that the 1st Respondent allegedly failed to specify the purpose(s) for which the Complainant's personal data was being processed during the pre-employment phase; and*

b. *Allegation 2 - that the Company allegedly processed personal data in a manner that is incompatible with the purposes for which the personal data was collected during the pre-employment application process*

130. The Office considered both allegations jointly as they are closely related. Section 30(1)(b)(i) of the Act provides for the lawful basis of processing and specifically provides that a data controller or data processor shall not process personal data, unless it is for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract.

131. The Complainant alleges that prior to the start date, the 1st Respondent's Office Administrator, reached out to the Complainant on 3rd August 2021 and requested for various personal documents particulars of which included: marriage certificate, birth certificates of the Complainant's children, copy of the Complainant's national identity card, copy of the Complainant's passport, copy of the Complainant's KRA PIN Certificate, NSSF and NHIF Number and her banking details.

132. Further, the Complainant alleges that when the Administrator asked the Complainant for the personal information on 3rd August 2021 there was no contract in place and the Complainant's start date was 16th August 2021, the date which the employment contract became effective. The Complainant also reiterates that neither was the purpose of collecting her personal and sensitive data nor her rights were communicated.

133. From the investigations, the Office finds that the 1st Respondent had the Employee privacy notice EMEA region on their website which shows the various information that the company collects from their employees. For instance, under clause 1 which provides for: *'What personal data do we collect about you'* provides that general, identification and contact information such as contact details including name, work, home address, telephone numbers, email address and emergency contact details, nationality, date of birth, gender, information on partners, family members and defendants, passport data is required.

134. Moreover, the 1st Respondent's privacy notice under clause 2 provides for: *'For what purposes do we use your personal data, and why is it justified?'* which clearly spells out the specific and legitimate purposes for which it processes personal data. They include: staff administration, such as managing work activities and personnel generally, including hiring and onboarding of employees; maintaining business operations, such as operating and managing technology and communication systems; emergencies and communications, such as facilitating communication between employees within the BD Group and/or with third parties as is necessary for business purposes and global initiatives; ensuring compliance, such as complying with BD policies and with local requirements, such as income tax and national insurance deductions; and health risk appraisals, which are only

conducted as permitted and/or required by local law for the sole purpose of managing the employment relationship.

135. The 1st Respondent also produced its Associate Handbook as evidence. The Associate Handbook guides the company on the rules and regulations as well as terms of conditions of employment.

136. From the above, it can be deduced that the 1st Respondent had the legitimate expectation that the Complainant's personal data collected pre-employment phase was relevant for the purposes of verifying the accuracy of the Complainant's details, supporting and fulfilling the employment contract as a HR requirement during the pre-employment application process. Furthermore, the Complainant did not have an issue with the same until the termination of her employment contract.

137. In light of the above, the Office finds that all the information that the Complainant gave to the 1st Respondent during the pre-employment phase was processed lawfully processed in line with section 30(1)(b)(i) of the Act and the Complainant has not adduced evidence to the contrary.

c. *Allegation 3 - that the Company allegedly failed to provide a valid explanation for the processing of the Complainant's personal data relating to their private or family affairs contrary to Section 25(e) of the Data Protection Act*

138. Section 25(e) of the Act provides that every data controller or data processor shall ensure that personal data is collected only where a valid explanation is provided whenever information relating to family or private affairs is required.

139. The Complainant alleges that prior to the start date, the 1st Respondent's Office Administrator, reached out to the Complainant on 3rd August 2021 and requested for various personal documents particulars of which included her marriage certificate and birth certificates of the Complainant's children and avers that neither the purpose of collecting her personal and sensitive data nor her rights were communicated.

140. The 1st Respondent's Employee Privacy Notice, explains that the 1st Respondent collects personal data including personal data of family members and dependants for the purpose of administering and providing benefits and other-work related

allowances to the Complainant and her family. This explanation is contained under clause 2 *'For what purposes do we use your personal data, and why is it justified?'* – Staff administration clause under the Employee Privacy Notice.

141. The Office therefore finds that the Complainant's personal data was lawfully processed by the 1st Respondent as the Complainant did not adduce any evidence to the contrary.

d. *Allegation 4 – that the Company allegedly failed to obtain consent for the transfer of the Complainant's line from the Company's account back to the Complainant after her contract with the Company had been terminated*

142. Section 30 (1) of the Act provides that a data controller or data processor shall not process personal data, unless the data subject consents to the processing for one or more specified purposes.

143. The Complainant alleged that the 1st Respondent through its agent gave instructions and authorized the 2nd Respondent to carry out registrations of the Claimant's private mobile number/SIM card, provided copies and details of her national ID card, and together with the 2nd Respondent, the 1st Respondent went to the extent of deciding the choice of tariff the Claimant should be put on for her private/personal SIM card without her prior informed consent.

144. The Complainant avers that the role of the 1st Respondent as a data processor should have ended upon termination of any agreement that 1st and 2nd Respondent regarding her corporate line. The Complainant further avers that even in cases where there is the option of online registration without having to visit the telecommunication operator store, the data subject who is the National Identity Card owner would be required to fill out the registration details on their own and upload their own identification documents for registration and verification/self-attesting.

145. From the investigations, the Office finds that the 1st Respondent's mobile phone policy guide provides that an associate is entitled to receive a mobile phone according to the stipulations of the policy. The policy further stipulates that sim cards registered under the 1st Respondent shall remain property of the 1st

Respondent unless surrendered to the associate upon exit or withdrawal from the mobile telephone services.

146. The 1st Respondent avers that the as a result of the aforementioned policy, the Complainant was taken through the options available to her. Pursuant to the 1st Respondent's Mobile Phone: Appropriate Use clause, paragraph 3, the issuance of a SIM Card happens in one of two ways; one - the Company procures the SIM card on behalf of the employee, or two - an employee is given the option of transferring their personal line to the Company's account with 2nd Respondent. In the Complainant's case, she chose the latter and opted to keep her personal line, mobile number +25473********, and to have the same transferred to the 1st Respondent's account with the 2nd Respondent. The 1st Respondent adduced the Number Porting Request Form and Email correspondence between the 1st Respondent's representative and 2nd Respondent with the subject line ('New Entrant Activation – Catherine Murithi').

147. From the evidence adduced, on 30th September 2024, the Complainant's employment was terminated by the Company on account of redundancy. As part of her offboarding process, the Company required her SIM card to be taken off its corporate account with Safaricom since she was no longer an employee of the Company, and thus, was no longer entitled to employee benefits. To that effect, on 3rd October 2024, the Company through one of its representatives, shared the Complainant's name and national identification card number with a representative from the 2nd Respondent informing them that the complainant was no longer an employee of the company, and as such, they should help in transferring the line, including the accumulated Bonga points, from the company's account to the complainant's personal account. The email was titled, "Exit Notice-Catherine Murithi. "The Complainant was also copied to that email.

148. On the same date the 3rd October 2024, the 2nd Respondent notified the 1st Respondent that they had successfully terminated the line. The email read as follows:

*"Hi M****,*

We have successfully terminated the line. For transfer to Catherine's ID, please share the copies."

149. From, the above, the 2nd Respondent can be seen to be requesting for the Complainant's ID in order to effect the transfer to the Complainant after the deactivation of the SIM card from the corporate account had been completed. The 1st Respondent then went ahead and shared a copy of the Complainant's ID and this time the Complainant was not in the copy of the said email. The Complainant only got to know of the same vide an email dated 4th October 2024 from the 2nd Respondent which read as follows:

*"Hi M*****,*

This is to confirm the transfer to Catherine's ID as shared in other mail was completed."

150. From the above and the investigations conducted, the Office concludes that the Complainant's personal data, that is, her ID number was lawfully processed in the process of deactivation of the Complainant's SIM card from the 1st Respondent's corporate account as evidenced by the email above. However, the 1st Respondent through sharing a copy of the Complainant's Identity Card with the 2nd Respondent without her consent points to unlawful processing of the Complainant's personal data.

151. Additionally, the 1st Respondent after termination of the Complainant's employment contract relied on its legitimate interest under Section 30(1)(b)(vii) as a lawful basis for processing the Complainant's personal data when it came to deactivation of the SIM card from the corporate account. However, the act of sharing the copy of the Complainant's ID without her consent in order to transfer the SIM card, the accumulated bonga points to the Complainant's personal account constitutes unlawful processing. In other words, processing of any details regarding the Complainant's private mobile number/SIM card registration, sharing of national ID copies/details and subsequent choice of tariff should have been handled by the Complainant who is the identity card holder or intended subscriber.

152. With regards to the **2nd Respondent**, the 1st Respondent notified them of the Complainant's exit from the 1st Respondent's entity *vide* an email dated 3rd October 2024 when facilitating the deactivation process. However, a representative from the 2nd Respondent still went ahead and requested the 1st Respondent to share a copy of the Complainant's ID.

153. On account of the transfer of the SIM card and the bonga points to the Complainant's personal account and without going to the lawfulness thereof, the Kenya Information and Communications (Registration of Sim-Cards) Regulations and specifically Regulation 10 on the transfer of SIM cards provides for the subscriber will be the one to provide a copy of their ID. In that regard, the 2nd Respondent ought to have requested the Complainant of a copy of her ID card as opposed to requesting the same from the 1st Respondent.

154. Additionally, the 2nd Respondent claims to have acted on the basis of the employment contract between the Complainant and the 1st Respondent but still proceeded to process her personal data without her consent after the employment contract had been terminated. Notably this employment contract has no mention of how 1st Respondent was to utilize the Complainant's personal data including her ID. Therefore, 1st and 2nd Respondent should have sort consent from the Complainant knowing that they were processing her data outside the said employment contract. Further, the 2nd Respondent failed to require the Complainant to appear in person and issue her consent during the registration of the transferred BD billed number to the Complainant's Identity card (as required by the law) under the Safaricom's Uwezo tariff.

155. To that extent, the 1st and 2nd Respondent are found liable for unlawfully processing the Complainant's personal data without her consent. Further, the Respondents did not establish other lawful basis that could override the data subject's consent when it came to processing of her personal data in line with section 30(1) of the Act.

e. Allegation 5 - that the Company allegedly transferred the Complainant's personal data outside of Kenya without proof of data protection safeguards or consent from the Complainant

156. Section 25(h) provides that every data controller or data processor shall ensure that personal data is not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

157. Moreover, Section 48(c)(vi) of the Act further provides that a data controller or data processor may transfer personal data to another country only where for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

158. Further, Regulation 40 of the Data Protection (General) Regulations (the General Regulations),2021 provides that data controller or data processor who is a transferring entity shall before transferring personal data out of Kenya ascertain that the transfer is based on (a) appropriate data protection safeguards; (b) an adequacy decision made by the Data Commissioner; (c) transfer as a necessity; or (d) consent of the data subject.

159. Furthermore, Regulation 41 of the General Regulations states that the requirement for appropriate safeguards is met where there is a legal instrument containing appropriate safeguards equivalent to the Act or where the data controller has assessed all the circumstances surrounding the transfer and concluded there are appropriate safeguards.

160. The Complainant also alleged that the 1st Respondent transferred her personal data outside of Kenya without her consent or proof of data protection safeguards. She alleges that such transfer of her personal data was effected through the copying in of two South African based colleagues to the 1st Respondent's email to the 2nd Respondent dated 3rd October 2024.

161. The 1st Respondent adduced evidence to show that the concerned employees who had been copied in the same email and reside in South Africa, are also subject to the same 1st Respondent's Employee Privacy Notice which requires

organisational safeguards such as the training of employees on how to handle personal data. Further, the 1st Respondent noted that by copying in two of the South Africa based colleagues in the email to Safaricom was necessary because they were part of the Local Finance team in Kenya, even though they were based in South Africa. Their involvement was crucial for financial matters related to the Kenyan office, and that is why they were copied in the email in the first place.

162. The Office therefore finds that Section 48(c)(vi) has been met as the 1st Respondent has proven compelling legitimate interests in processing the complainant's personal data as the other employees were also in copy of the said email.

163. The Office also takes cognizance of the Protection of Personal Information Act which covers issues of data protection in South Africa which meets the parameters set under Regulation 41 of the General Regulations.

164. In this respect, the requirements of the Act and the General Regulations, have both been met by the 1st Respondent.

f. Allegation 6 – that the Company allegedly failed to report an alleged data breach to the ODPC within seventy-two hours

165. Section 43 of the Act provides that where personal data has been accessed or acquired by an unauthorized person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorized access, a data controller shall notify the Data Commissioner without delay, within seventy-two hours of becoming aware of such breach.

166. From the evidence adduced by the Complainant, the Office holds that there was no data breach as the complaint at hand has been processed in line with section 56 of the Act and the Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021.

III. WHETHER THERE WAS A VIOLATION OF THE COMPLAINANT'S RIGHTS UNDER THE ACT

167. Section 26(a) of the Act provides for the right to be informed of the use to which a data subject's personal data is to be put.

168. The 1st Respondent's actions by unlawfully disclosing the Complainant's copy of ID to the 2nd Respondent in a bid for the transfer to be effected to the Complainant's personal account once the deactivation from the corporate account had already been completed, also infringes on the Complainant's right to be informed under Section 26(a) of the Act.

169. The 2nd Respondent having been informed of the Complainant's exit from the 1st Respondent should have dealt with the intended subscriber directly by informing her why they needed the ID copies, collecting the ID copies from the data subject and conducting verification using the data subjects original ID card as well as obtaining accurate personal data directly from the data subject.

170. The Complainant had the right to be informed about how her personal data will be used by the 2nd Respondent. Instead, the 2nd Respondent opted to deal with the 1st Respondent and request for the Complainant's ID copies from the 1st Respondent while fully aware that the Complainant was no longer in any contractual relationship with the 1st Respondent.

171. From the foregoing, this Office finds that the Complainant's right to be informed under Section 26(a) of the Act was violated by the Respondents.

IV. WHETHER THE COMPLAINANT IS ENTITLED TO ANY REMEDIES UNDER THE ACT AND THE ATTENDANT REGULATIONS.

172. Pursuant to Regulation 14 (2) of the Enforcement Regulations, a determination shall state the remedy to which the complainant is entitled. The remedies are provided for in Regulation 14 (3) of the Enforcement Regulations.

173. The Complainant requested this Office to issue various declarations relating to the violation of the Constitution of Kenya, 2010. The Office has already concluded that it doesn't have jurisdiction over the same. Further, the Complainant sought for a permanent injunction against the Respondent which the Office finds that it does not have jurisdiction to entertain.

174. The Complainant also requested this Office to issue an award of compensation. Section 65 of the Act provides that a person who suffers damage by reason of a

contravention of a requirement of the Act is entitled to compensation for that damage from the data controller. The Section indicates that damage included financial loss and damage not involving financial loss including distress.

175. Further, Regulation 14 (3) (e) of the Enforcement Regulations provides that the Data Commissioner may make an order for compensation to the data subject by the Respondent.

176. In considering whether to issue compensation, this Office takes into consideration the fact that the Complainant's right under Section 26 (a) were infringed upon by the Respondents and the processing of the Complainant's personal data without consent.

177. Furthermore, the Complainant requested to be awarded specific damages of Kenya Shillings Two Hundred Thousand (KES 200,000) which was particularized as Advocates invoice. However, the Office declines to award the same as no proof of payment was adduced as evidence.

178. In this context, the 1st and 2nd Respondents are hereby ordered to pay the Complainant **Kenya Shillings Two Hundred and Fifty Thousand Shillings each (KES. 250,000)** for the infringement of her rights under the Act and for the unlawful processing of her personal data without her consent.

VI. FINAL DETERMINATION

179. The Data Commissioner therefore makes the following final determination;

i. The Respondents are hereby found liable for infringement of the Complainant's rights right to be informed under Section 26(a) of the Act and for the unlawful processing of the Complainant's personal data without her consent.

ii. The 1st Respondent to pay the Complainant a sum of **Kenya Shillings Two Hundred and Fifty Thousand (KES 250,000)** as compensation.

iii. The 2nd Respondent to pay the Complainant a sum of **Kenya Shillings Two Hundred and Fifty Thousand (KES 250,000)** as compensation.

iv. The 1st Respondent is hereby ordered to register as a data controller in Kenya.

v. Parties have the right to appeal this determination to the High Court of Kenya within thirty (30) days.

DATED at **NAIROBI** this 24th day of February 2025.

IMMACULATE KASSAIT, MBS
DATA COMMISSIONER