REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

ODPC COMPLAINT NO. 1159 OF 2024 CONSOLIDATED WITH ODPC COMPLAINT NO. 1160 OF 2024 AND ODPC COMPLAINT NO. 1161 OF 2024

BHARAT THAKRAR.....COMPLAINANT

-VERSUS-

WPP SCANGROUP PLC.....1ST RESPONDENT

WPP PLC.....2ND RESPONDENT

CONTROL RISKS GROUP.....3RD RESPONDENT

DETERMINATION

(Pursuant to Section 8 (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 relates to the alleged multiple breaches of the Complainant's privacy and data protection rights by the 1st, 2nd & 3rd Respondents. This includes the 1st, 2nd & 3rd Respondent's failure to give effect to the Complainant's data subject rights and failure to comply with their legal obligations.

B. LEGAL BASIS

2. Article 31 (c) and (d) of the Constitution of Kenya, 2010 provides for the right to privacy. Consequently, as an effort to further guarantee the same, the Data Protection Act, 2019 (hereinafter 'the Act') was enacted.

3. The Office of the Data Protection Commissioner (hereinafter '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 (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) 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.

C. BACKGROUND OF THE COMPLAINTS

5. The Office received three complaints by Bharat Thakrar (hereinafter 'the Complainant') all dated 31st July, 2024 pursuant to Section 56 of the Act and Regulation 4 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 (hereinafter the 'Enforcement Regulations'), against the 1st, 2nd & 3rd Respondents. The complaints were consolidated with the consent of the Complainant.

6. WPP Scangroup PLC (hereinafter 'Scangroup' or '1st Respondent') is a public limited liability company specialising in marketing services and headquartered in Nairobi, Kenya. Scangroup is a subsidiary of WPP PLC (hereinafter 'WPP' or 2nd Respondent), a British multinational communications, advertising, public relations, technology, and commerce holding company headquartered in London, England. Control Risks Group (hereinafter 'CRG' or 3rd Respondent) is a risk and strategy consulting firm headquartered in London, England. Jointly, they will be referred to in this Determination as 'the Respondents'.

7. The Complainant is the former Chief Executive Officer (CEO) and Director at Scangroup. He is a shareholder at Scangroup.

8. Pursuant to Regulation 11 of the Enforcement Regulations, the Office, notified the 1st, 2nd & 3rd Respondents of the complaint filed against them *vide* a Notification Letters dated 7th August 2024 and referenced ODPC/CONF/1/5/VOL II (85), ODPC/CONF/1/5/VOL II (86) and ODPC/CONF/1/5/VOL II (84) respectively, and required their response within 21 days. In the notification of the complaints filed against the 1st, 2nd & 3rd Respondents, they were to provide-

    a. A response to the allegations made against them by the Complainant;
    b. Any relevant materials or evidence in support of the response;
    c. The lawful basis relied upon to process the Complainant's personal data;
    d. Details on how they obtained each of the Complainant's documents referred to in his access request forms;
    e. Evidence as to whether the Complainant consented to the processing of their personal data in relation to the investigations done;
    f. The mitigation measures adopted or being adopted to address the complaint to the satisfaction of the Complainant, if any;
    g. A demo of how they fulfil the rights of a data subject; and
    h. Any other information they wish the Office to consider.

9. On 15th August 2024, the 1st & 2nd Respondents though their advocates on record, Coulson Harney LLP, responded to the said notification. In their responses, the 1st and 2nd Respondents requested that the complaint be resolved through alternative dispute resolution (ADR).

10. As the ADR process is voluntary, this Office requested for the Complainant's consent to resolve the dispute through ADR. The Complainant declined to give his consent to resolve the dispute through ADR though a letter dated 27th August, 2024 Ref No. 5/4215/003.

11. The Complaint then fell for determination by this Office as per Regulation 15 (8) of the Enforcement Regulations which provides that where the complaint is not determined through ADR, the Data Commissioner shall proceed to determine the complaint as provided for in the Act and the Regulations.

12. The 1st & 2nd Respondents responded to the complaint and the notification of complaint letter *vide* letters dated 15th August, 2024; 27th August, 2024; 28th August, 2024 and 12th September, 2024.

13. The 3rd Respondent responded to the complaint and the notification of complaint letter *vide* letters dated 19th August, 2024, 16th September, 2024 and 8th October, 2024.

14. In addition to the complaint, the Complainant filed a written statement in support of the complaint dated 17th September, 2024 and two letters filed on his behalf by his advocates. Triple OK Law Advocates, both dated 5th September, 2024.

15. This determination is therefore as a result of analysis of the aforementioned documents and investigations conducted by the Office.

D. NATURE OF THE COMPLAINT

I. SUMMARY OF THE COMPLAINANT'S CASE

16. The Complainant stated that he lodged the complaint against the Respondents alleging breach of his constitutional right to privacy guaranteed under Article 31 of the Constitution and breach of his rights as a data subject as provided in the Act, through unlawful and unjustified processing of his personal information. According to him, these breaches caused him profound personal and professional harm.

17. The Complainant posits that he founded Scanad Marketing Limited ('Scanad') in 1982 and managed to grow it into a major advertising agency in East Africa. By 2005, Scanad had evolved into Media Initiative East Africa Limited. In the same year, following a restructuring, it was renamed Scangroup PLC. In 2006, Scanad evolved into WPP Scangroup Plc and is now listed on the Nairobi Securities Exchange. Upon listing, the Complainant was employed as Director and Chief Executive Officer of Scangroup PLC effective 1st October, 2005 pursuant to a contract of employment dated 5th December, 2005.

18. He asserts that WPP is a significant shareholder in Scangroup and that CRG was engaged as a third party by WPP and Scangroup to access his personal information. According to him, during their involvement, CRG unlawfully accessed and processed his personal data without a legitimate basis or his consent.

19. The Complainant alleges that WPP as the largest shareholder of Scangroup played a significant role in the governance and decision making processes within Scangroup, thereby influencing the processing activities of Scangroup, effectively acting as data controller.

20. According to the Complainant, CRG was utilized to access his laptop and other personal data, both physically and as backed up on cloud. This was done without his knowledge and consent and included data unrelated to his work responsibilities such as iCloud data containing personal WhatsApp messages. CRG thereafter compiled a report based on their investigations. This report was shared with the Capital Markets Authority (CMA), WPP and Scangroup.

21. The Complainant alleges that Scangroup and WPP's failure to provide transparency, safeguard his personal data, and involve him in the process of investigations by CRG resulted in significant professional and personal harm. His personal data was mishandled and improperly shared among these entities during the investigations.

22. The Complainant contends that WPP as the parent company exercises significant control over the subsidiary's operations and has failed to implement adequate safeguards and controls over its subsidiary's data processing activities, leading to the breach and must be held accountable for the breaches of his data protection rights.

23. According to the Complainant, in 2021, he was suspended from his position as Chief Executive Officer of Scangroup following allegations of misconduct and notified of disciplinary proceedings against him and requested to attend a hearing. This suspension led to his resignation under duress.

24. The Complainant states that despite his resignation, Scangroup and WPP continued to disclose adverse personal data about him to the CMA, raising questions regarding the appropriateness and legality of such disclosures post-employment termination by way of resignation.

25. The Complainant maintained that his data subject rights are not restricted to other judicial processes and that there is no limitation or exemption provided either in the Constitution or in legislation subrogating his right to seek protection and relief with respect to breaches arising from violation of his personal data to other legal processes.

26. The Complainant posits that the breaches by the Respondents have caused him considerable financial loss, emotional turmoil and reputational harm, significantly impacting his business, income, mental health and professional standing.

Complaint against the 1st Respondent (Scangroup)

27. The grounds for the complaint against the 1st Respondent are as follows –

(a) *Denial of access in breach of the Complainant's right as a data subject* – That Scangroup has systematically denied the Complainant's requests for access to crucial personal data without sufficient justification. The Complainant alleges that Scangroup improperly withheld access to logs and records, claiming inability to comply with the detailed requests for data extraction and citing lack of access to logs and records. According to the Complainant, Scangroup failed to respond to specific queries regarding the scope and nature of personal data processing activities, thereby obstructing his right to fully understand how his data was being processed.

(b) *Improper invocation of exemptions and general situations* – That Scangroup has based the denial of access to the requested documents and information on the grounds of public interest without having met the required threshold. According to the Complainant, there is no significant public interest in withholding his personal information as it does not

relate to national security, public safety or other critical public concerns and that the public interest exemption should not be used to obscure transparency and accountability in the handling of personal data.

(c) *Data sharing and third-party disclosures* – That CRG commissioned by Scangroup and WPP accessed and processed the Complainant's personal data from the company-issued devices including iCloud data and private WhatsApp messages unrelated to company responsibilities, without his consent or lawful basis. The Complainant contends that Scangroup breached his rights by denying his request to access detailed personal data regarding the data points and procedures used to collect and analyse his personal data, specifically concerning company-provided devices, including access logs and data extraction details. The Complainant relied on the Act, the Constitution and European Data Protection Supervisor (EDPS) guidelines on transparency and accountability when accessing employees' personal data.

(d) *Unauthorised disclosure to majority shareholder* – That Scangroup disclosed the Complainant's personal data, including details of disciplinary procedures and correspondences with WPP's legal counsel post-employment without obtaining his consent.

(e) *Employment and investigative data* – The Complainant alleged that Scangroup denied his request to access his personal data held by the company and that the claim that the request was manifestly excessive is not supported by the Act.

(f) *Continued disclosure of adverse personal information* – The Complainant states that Scangroup denied his request to access detailed personal data regarding the sharing of his personal data with third parties including the specific purposes of such sharing and the legal basis upon which these activities were predicated. The Complainant relied on the Act, the Constitution and European Data Protection Supervisor (EDPS) guidelines on transparency in data sharing practices.

(g) *Lack of transparency and accountability* – The Complainant asserts that Scangroup have not provided clear explanations or documentation supporting their decisions to deny access to specific categories of personal data and that there is no evidence of proper record keeping or documentation regarding the processing of his personal data.

(h) *Misapplication of legal privilege, confidentiality and public interest* – According to the Complainant, the Respondents' invocation of confidentiality and public interest under Regulation 56 as grounds for denial is legally baseless. The Complainant asserts that the requested personal data, especially those contained in investigative reports and communications with external entities such as CRG do not fall within the scope of legal privilege. The reports are likely to include factual findings and personal data processed during investigations, which do not inherently involve confidential legal advice or preparation for litigation.

(i) *Impact on rights and obligation* – The Complainant avers that the denial of access to his personal data and the unauthorised access of his personal data by third parties has had a detrimental impact on his rights. This includes damage to his professional and personal reputation and standing within regulatory bodies such as the CMA based on undisclosed adverse information and potential legal repercussions stemming from Scangroup's mishandling and unauthorized disclosure of his personal data which could affect his future career prospects and personal and family's wellbeing.

28. The legal basis for the Complaint against the 1st Respondent include –

i. Breach of right to access.
ii. Breach of his constitutional right to privacy.
iii. Breach of Data Protection Act right to privacy.
iv. Unauthorised access and processing of personal information.
v. Data minimization and Purpose Limitation.
vi. Security measures and breach notification.
vii. Data protection by design and default.

viii. Misapplication of legal privilege, public interest and confidentiality.

ix. Third party disclosure without consent.

x. Transparency and fair processing.

xi. Continued disclosure of adverse personal information.

xii. Invalid claim of manifestly excessive request.

Complaint against the 2nd Respondent (WPP)

29. The grounds for the complaint against the 2nd Respondent were as follows –

(a) *Unauthorised data processing and access* – The Complainant states that WPP commissioned a third party, CRG, to access and investigate the Complainant's personal data without his express consent. The Complainant states that WPP should have implemented measures to segregate personal data from work related data to protect his privacy, thereby disregarding the principles of data minimization and necessity as outlined in the Act.

(b) *Use of personal data beyond original scope* – That the Complainant's personal data initially collected by Scangroup for employment purposes was subsequently used by WPP for investigations without informing him or obtaining his consent. The Complainant states that the data was shared with CMA and the usage goes beyond the original scope of data collection violating the principle of purpose limitation.

(c) *Denial of access to personal data* – That WPP has persistently denied the Complainant's requests for access to crucial personal data without justification, despite having sent a DSAR. The Complainant contends that WPP failed to respond to specific requests regarding the scope and nature of personal data processing activities, thereby obstructing his right to fully understand how his data has been processed.

(d) *Improper invocation of exemptions and general situations* – That WPP has based the denial of access to the requested documents and information on the grounds of public interest. According to the Complainant, there is no significant public interest in withholding his

personal information as it does not relate to national security, public safety, or other critical public concerns.

(e) *Employment contract and investigative data* – That WPP falsely claimed to have the Complainant's employment contract, despite Scangroup confirming in writing that his employment contract is held by WPP in London.

(f) *Claims of legal privilege, confidentiality and public interest* – That WPP has invoked legal privilege, confidentiality and public interest to deny his access requests to his personal data. The Complainant state that the investigation reports and communication with external entities like CRG and CMA likely contain factual findings and his personal data which are not inherently covered by legal privilege or involve confidential legal advice or preparation for litigation. The Complainant posits that WPP was not engaged in a transparent process and that instead of addressing specific confidentiality concerns through redaction or partial disclosure, they have wholly denied his request, further demonstrating the lack of accountability. He further states that Regulation 55 and 56 should not be manipulated as a blanket exemption from all the provisions of the DPA. The principles of data processing and especially data subject rights must still apply and the Respondents have not demonstrated compliance with the principles even when relying on the exemption.

(g) *Inadequate response to DSAR* – That despite submitting a DSAR on 26th April, 2024, WPP failed to provide the requested information thereby preventing the Complainant from understanding the full extent of how his personal data was processed and shared.

(h) *Lack of transparency and accountability* – That at no point was the Complainant informed of the nature and extent of data sharing and processing conducted by WPP. That the processing was carried out without his explicit consent, violating his rights under Section 26 of the Act.

(i) *Improper personal data sharing with third parties* – That WPP involved third parties like CRG in processing his personal data without a legal basis.

30. The legal basis for the Complaint against the 2nd Respondent include –

(a) Breach of his right of access to his personal data.

(b) Breach of his constitutional right to privacy.

(c) Breach of the Data Protection Act.

(d) Misapplication of legal privilege, public interest and confidentiality.

(e) Breach of transparency and data security obligations.

(f) Invalid claim of manifestly excessive request.

(g) Misrepresentation and misleading statements

Complaint against the 3rd Respondent (Control Risks Group (CRG))

31. The grounds for the complaint against the 3rd Respondent are as follows –

(a) *Unauthorised data processing and access* – The Complainant states that CRG unlawfully accessed and processed his personal data without his consent which included data from his devices and cloud storage containing private communications unrelated to his professional responsibilities. According to the Complainant, while accessing work related data may be justified for specific purposes, the unauthorized access and processing of his personal WhatsApp messages constitutes a severe breach of privacy.

(b) *Denial of access to personal data* – The Complainant asserts that despite his DSAR, CRG did not provide access to crucial personal data, including the investigation report it compiled, which potentially contains adverse information impacting his standing with regulatory bodies. CRG failed to respond to specific queries regarding the scope and nature of personal data processing activities, thereby obstructing his right to fully understand how his data was being processed. The Complainant claimed that the grounds relied on by CRG that they were acting on instructions from their client, that they do not possess the Complainant's personal

data due to their data deletion policies, that fulfilling the DSAR would be disproportionate and costly and that his request was manifestly excessive, and were baseless.

(c) *Use of personal data beyond original scope* – That some of the Complainant's personal data initially shared with Scangroup in the scope of his employment was unlawfully processed by CRG for investigations and other purposes without informing him or obtaining his consent.

(d) *Claims of legal privilege and confidentiality* – That CRG has invoked legal privilege and confidentiality to deny the Complainant's DSAR thereby preventing him from verifying and understanding the personal data CRG processes about him and obstructing his rights as a data subject. The Complainant posits that the reports and documents likely contain factual findings and his personal data which are not inherently covered by legal privilege or involve confidential legal advice or preparation for litigation.

(e) *Inadequate response to DSAR* – That despite submitting his DSAR on 26th April, 2024, CRG failed to provide the requested information.

(f) *Lack of transparency and accountability* – The Complainant avers that CRG has not provided clear documentation or explanations for the processing activities involving his personal data. He was not informed of the nature and extent of data sharing and processing conducted by CRG. Investigations were carried out and a report prepared without his explicit consent.

32. The legal basis for the Complaint against the 3rd Respondent include –

(a) Breach of right to access (Section 26(b) of the DPA and Regulation 9 of the DP regulations)

(b) Breach of his constitutional right to privacy.

(c) Breach of the Data Protection Act.

(d) Misapplication of legal privilege, public interest and confidentiality.

(e) Invalid claim of manifestly excessive request.

II. SUMMARY OF THE 1ST & 2ND RESPONDENTS' RESPONSE

33. Scangroup and WPP *vide* responses dated 15th August, 2024; 27th August, 2024; 28th August 2024 and 12th September, 2024 and filed by their advocates on record, responded to the Complaint and the Notification letters.

34. In their response, Scangroup and WPP confirmed receipt of DSARs originating from the Complainant and dated 26th April 2024. They confirm responding to the DSARs *via* responses dated 3rd May 2024, within the statutorily defined seven days.

35. They assert that, as a preliminary issue, there is an ongoing litigation between Scangroup, WPP and the Complainant being *HCCOMM/E147/2024 – Bharat Kumar Thakrar Vs WPP Plc, WPP Scangroup Plc & 7 Others* ('the Suit').

36. They state that the Complainant filed Suit *via* a Plaint dated 22nd March 2024 claiming that the manner in which he left employment as a director and Chief Executive Officer of WPP Scangroup Plc was primarily due to collusion by Scangroup and WPP. They state that the Complainant has categorised his claim in the Suit into the following sub-headings: malice, discrimination, inducement, breach of contract and breach of fiduciary duties.

37. According to them, in paragraph 31 of the Plaint, the Complainant references his request to be furnished with a copy of a report containing the investigation of allegations against him and this assertion is identical to what is being sought by the Complainant from this Office. They aver that there is an overlap between the claims in the Suit and the requests in the DSARs and that the subject matter of the suit is directly relevant to the DSAR in view of the information requested.

38. They aver that the Suit is ongoing and that the DSARs appear to them to be a "fishing expedition" to circumvent the proper discovery process in the ongoing Suit which was initiated by the Complainant. They relied on the case of *Concord Insurance Company Limited v NIC Bank Limited [202] eKLR* on the importance of discover provisions and *Eliud Michael Sichei v Tutti Holdings Limited Company [2021] eKLR* on fishing expeditions as abuse of process.

39. In view of the Suit, it was Scangroup's and WPP's concern that any disclosure of information pursuant to the DSAR would seriously prejudice them and have a detrimental impact on the outcome of the litigation. They requested that the investigation of the Complaint by this Office be suspended or alternatively dismissed pending the outcome of the Suit in view of the *sub judice* rule as the matters pending before court inevitably touch on issues currently before this Office for determination.

40. On the facts leading to the complaint, Scangroup and WPP state that sometime in late 2020 serious allegations were levelled against the Complainant alleging that he had engaged in behaviour and practices amounting to gross misconduct, contrary to the terms of Scangroup's policies and procedures, its Code of Business Conduct and Board Charter. The allegations were made through whistle-blower reports of employees and former employees of Scangroup using the "Right to Speak Line", which allegations were then shared with Scangroup's board of directors.

41. They assert that on 18th February 2021, the Complainant was suspended to pave way for the investigation and Scangroup, through CRG, commissioned a comprehensive investigation into the allegations made against the Complainant.

42. Following the outcome of the investigations, Scangroup state that they issued the Complainant with a Notice to Show Cause (the NTSC) dated 16th March 2021 setting out the acts which amounted to gross misconduct by the Complainant with a request for the Complainant to provide an explanation for the allegations against him.

43. According to Scangroup and WPP, instead of responding to the NTSC, the Complainant voluntarily resigned as a director and the Chief Executive Officer of Scangroup on 23rd March 2021.

44. As regards communication with the CMA, Scangroup and WPP posit that any communications by Scangroup are in line with its legal reporting requirements as a listed company pursuant to the Capital Markets Act and corresponding regulations.

45. With respect to the lawful bases relied upon by them to process the Complainant's personal data, they state that in light of the employer-employee relationship that existed between the Complainant and Scangroup, the lawful bases upon which they processed the Complainant's personal data include processing necessitated for the performance of employment contract, performance necessary for compliance with legal obligations (for example, the Employment Act requires employers to keep written particulars of employment for a period of five years after the termination of employment), as well as in pursuit of the protection of their legitimate interests especially in the context of investigations into the conduct of the Complainant during the course of his employment.

46. They state that any and all of the Complainant's referenced documents, which are in their possession, have been received in the context of the Complainant's employment and any further processing was carried out in accordance with Scangroup's rights as an employer.

47. Further, they posit that Section 28 of the Act allows the indirect collection of personal data where such collection is necessary for the prevention, detection, investigation, prosecution and punishment of crime; and/or for the protection of the interests of the data subject or another person. In the context of the disciplinary investigations against the Complainant, they had a legal basis for not relying on the Complainant's consent as the basis for processing the Complainant's personal data.

48. They aver that there was no malice nor conspiracy in the actions that led to the Complainant's voluntary resignation.

49. In response to the Complainant's grounds for the complaint against them, Scangroup and WPP, state as follows –

    (a) *Unauthorised data processing and access* – Scangroup and WPP maintain that the information requested by the Complainant is legally privileged and it would prejudice the ongoing Suit. They state that the DSAR is frivolous and vexatious and submitted in bad faith. Regarding

the Complainant's request for copies of the relevant data protection policies that were in force between November 2019 to March 2021, the Complainant, being the CEO of Scangroup, would have been responsible for signing off and effecting the WPP Data Privacy & Security Charter. That the Complainant attended data protection and security trainings and he was aware of the WPP Data Privacy and Security Charter which applied at a group level on all operating entities. They state that a soft copy of the Complainant's redacted HR file was delivered to the Complainant electronically on 27th August 2024.

(b) *Improper invocation of exemptions and general situations* – Scangroup and WPP assert that they are permitted to rely on the general exemptions provided under Section 51 (2)(b) of the Act, Regulation 55 (a) and Regulation 56 (b) & (d) of the Data Protection (General) Regulations, 2021 and that the Complainant's interpretation of public interest in the context of a DSAR is therefore misguided.

(c) *Data sharing and third-party disclosures & unauthorised disclosures* – It is Scangroup's and WPP's position that an extract of Clause 8 of the Complainant's Service Contract sets out how the Complainant's data was handled during the course of his employment and the WPP Data Privacy & Security Charter outline the 1st & 2nd Respondent's rights as regards data sharing. They state that no sensitive personal data of the Complainant was processed by them in the manner alleged and consequently, consent was not required. They further took issue with the Complainant's reliance on the EDPS guidelines.

(d) *Employment and investigative data* – They assert that this information is protected by legal privilege and they reserve their rights in relation to such information. Scangroup and WPP stated that this information can be requested through a disclosure request in the course of the ongoing suit between themselves and the Complainant.

(e) *Continued disclosure of adverse personal information* – Scangroup and WPP reiterated their response to the DSAR and further took issue with the Complainant's reliance on the EDPS guidelines. They stated that they are required to legally retain employee data post termination of employment, for example, the Employment Act requires employers to keep written particulars of employment for a period of five years after the termination of employment. Additionally, they aver that the WPP Data Handling and Retention Policy, sets out their data retention policies and practices and that this was undertaken in line with the objectives in Clause 8 of the Complainant's Service Contract. Disclosures to CMA were subject to statutory reporting requirements under the Capital Markets Act.

(f) *Lack of transparency and accountability / Use of personal data beyond original scope* – They stated that the Complainant was the former CEO of Scangroup and had full visibility of the data protection policies introduced. They further state that as a listed company and a licensee of the CMA, Scangroup is under a strict legal requirement to maintain its books, records, accounts and audits and regularly report its affairs to the CMA in line with the provisions of the Capital Markets Act. They referred to the contents of WPP Data Privacy & Security Charter with respect to their policies and practices in the context of disclosure of employee personal data, including in the context of disciplinary investigations.

(g) *Misapplication of legal privilege, confidentiality and public interest* – Scangroup and WPP stated in response that concept of legal privilege, provided for in Sections 134 to 137 of the Evidence Act and is aimed at protecting the client to whom legal services are provided. They relied on the decisions in *Total Security Limited & another v Teleposta Pension Scheme & 8 others (Tribunal Case BPRT/903/2016 of 2016) [2022] KEBPRT 693 (KLR) (Civ) (9 September 2022)* (Ruling) and *Manani Lilan & Mwetich Co Advocates v Veronica Sum [2022] eKLR.* They state that they are under no legal obligation to provide explanations as to why

certain information/documents are protected by legal privilege and attendant confidentiality when these are rights that automatically arise with respect to information/documents exchanged between themselves and their professional advisors. According to Scangroup and WPP, it is challenging and nearly impractical for them to provide explanations to the Complainant regarding the nature of information requested that are covered by legal privilege without jeopardising the legal privilege covering such information.

(h) *Impact on rights and reputation* – Scangroup and WPP emphasised that at no point did they make any information regarding the Complainant's resignation or the Suit public.

(i) *Inadequate response to DSAR* – They maintained that WPP has responded to the DSAR in good faith as per the response dated 3rd May 2024. They reiterated that the DSAR was vague, broad, and excessive. There was no specificity with the request which appeared to be a fishing expedition. Furthermore, they assert that there is a disproportionate amount of repetition in the Complainant's DSAR as well as in the complaint which is convoluted in purpose. According to them, the elements of the Complainant's DSAR are manifestly unfounded and excessive as the Complainant clearly has no intention to exercise his rights in good faith and are being used to harass them.

III. SUMMARY OF THE 3RD RESPONDENT'S RESPONSE

50. CRG, *vide* responses dated 19th August, 2024; 16th September, 2024 and 8th October, 2024 confirmed having received a DSAR from the Complainant dated 26th April, 2024 and that they responded to the DSAR *via* email to the Complainant on 3rd May 2024, within the statutorily defined seven days.

51. CRG stated that the underlying complaint against them is directly related to two other complaints filed against the WPP and Scangroup who have petitioned the Office for advice and recommendations on how to respond to the Notifications of Complaint letters issued to them, given there is pending litigation between

the Complainant and WPP and Scangroup, i.e. *HCCOM/E147/2024 — Bharat Kumar Thakrar vs WPP Plc, WPP Scangroup Plc & 7 Others* (the Suit).

52. According to CRG, the personal data requested by the Complainant in the DSAR was processed by them solely in their capacity as data processor on behalf of Scangroup as the data controller, as defined under the Act.

53. CRG posits that the personal data requested by the Complainant in the DSAR directly pertains to the Suit and the Respondents herein believe that disclosure would seriously prejudice their rights as defendants and have a detrimental impact on the outcome of the Suit.

54. CRG states that on or about 19th February, 2021, they entered into a legally binding agreement with Coulson Harney LLP (t/a Bowmans Kenya), who acted as legal counsel to Scangroup to investigate allegations of serious misconduct against the Complainant who was Director and CEO of Scangroup. They assert that the agreement included specific written provisions, including instructions, for the processing of personal data, in accordance with Section 42 (2)(b) of the Act and Regulation 25 (3) of the General Regulations.

55. Per the agreement between CRG and Coulson Harney LLP, CRG acted as a data processor on behalf of its data controller, Scangroup, for the processing of personal data as part of the Investigation.

56. According to CRG, the Suit directly pertains to the circumstances of the Complainant's resignation, including the misconduct allegations against the Complainant which were the focus of the investigation.

57. CRG denied having illegally processed the Complainant's personal data. They state that the Complainant's personal data was provided to them by the data controller, Scangroup, and was processed solely in the context of the investigation under the instructions of Coulson Harney LLP through its client, Scangroup (the data controller).

58. According to CRG, as data processor they act upon the instructions of their data controller in accordance with the Act. They further state that the Complainant's strategy of issuing DSARs against the Respondents puts them, acting as data processor, in jeopardy of regulatory and contractual breach by failing to act in accordance with their data controller.

59. CRG assert that the personal data requested by the Complainant was solely processed in the context of the investigation and pertains to the Suit and that they acted in accordance with the instructions of WPP and Scangroup, including the data controller, to respond consistently and in accordance with their instructions. They aver that the parameters of the investigation determined why and how the Complainant's personal data was processed. They were engaged to provide services related to the investigation and instructed, as part of the services, to process the Complainant's personal data. CRG assert that they would not have processed the Complainant's personal data but for the instructions of Scangroup through Coulson Harney LLP.

60. CRG observe that the Complainant was able to and did raise a DSAR against the data controller meaning a DSAR against CRG as data processor was not the Complainant's only recourse for the exercise of his rights and if anything, is manifestly excessive and unfounded.

61. They further state that as their engagement for the investigation was with Coulson Harney LLP, acting as legal advisors to Scangroup, all investigative data, communications and reports specifically requested by the Complainant on the investigation are subject to legal privilege and confidentiality, contrary to the assertion of the Complainant.

62. CRG posits that their engagement was for the "provision of confidential and privileged legal advice" and that the investigative data and report provided to Coulson Harney LLP informed the legally privileged advice it gave to Scangroup on matters directly in issue in the Suit and is thus protected by legal privilege.

63. CRG states that as data processor, they rely on the lawful basis of the data controller, in accordance with the roles and responsibilities defined by the Act. That it would be contrary to their role as data processor to establish a legal basis separate from the data controller or to procure consent independently. Further, as they are not data controller, they are not vested with the authority to make determinations on restrictions of processing.

64. They further assert that per the definition of sensitive personal data in the Act, personal conversations, WhatsApp and iCloud data is not *prima facie* sensitive personal data.

65. It was CRG's request that the complaint against them be dismissed in its entirety or in the alternative, they request the suspension of the complaint against Control Risks pending this Office's decision on the Respondents' requests for suspension of the proceedings before this Office, particularly pending the outcome of the Suit in view of the *sub judice* rule as the matters pending before court inevitably touch on issues currently before this Office for determination.

E. SUMMARY OF EVIDENCE ADDUCED

I. THE COMPLAINANT'S EVIDENCE

66. As part of his evidence, the Complainant submitted the following documents:

a) Witness Statement of Bharat Thakrar dated 17th September, 2024.
b) Copies of the DSARs dated 26th April, 2024.
c) Copies of WPP's & Scangroup's responses to the DSARs dated 3rd May, 2024.
d) Copy of the suspension notice and suspension resolution.
e) Negative media stories published about the Complainant.
f) Redacted copy of the Notice to Show Cause.
g) As part of the exhibits sent to CMA two examples of private WhatsApp messages.
h) Copy of email dated 4.2.22.
i) Copy of letter dated 11.3.22.
j) Copies of correspondences between Anjarwalla & Khanna & CH Advocates.

k) Copy of letter from CMA confirming no regulatory breaches.

l) Unsigned Copy of his Service Contract with WPP Scangroup.

m) Copy of WPP Scangroup HR Policy.

II. THE 1ST & 2ND RESPONDENTS' EVIDENCE

67. As part of their evidence, the 1st & 2nd Respondents provided the following:

a) WPP Data Privacy & Security Charter.

b) The Complainant's certificate of completion of the WPP Privacy and Data Security Awareness Course.

c) An extract of the Complainant's service contract.

d) Copies of the DSARs dated 26th April, 2024.

e) Copies of WPP's & Scangroup's responses to the DSARs dated 3rd May, 2024.

f) Copies of Statements of Defence of WPP & Scangroup dated 22nd May, 2024.

g) Written statement of Scangroup Head of Legal and Data Protection Officer dated 24th October, 2024.

III. THE 3RD RESPONDENT'S EVIDENCE

68. As part of their evidence, the 3rd Respondent submitted a redacted copy of a Proposal for Investigation Support dated 19th February, 2021.

F. INVESTIGATIONS UNDERTAKEN

69. In exercising its investigative mandate under the Act, and upon review of the documentation submitted by the Complainant and the Respondents, this Office established that the investigation reports prepared by CRG in instructions from Coulson Harney LLP, acting on behalf of Scangroup were key documents for purposes of conducting a fair and effective investigation of the complaint.

70. This was premised on the allegation that these investigation reports may have contained the Complainant's personal data and sensitive personal data and that the same was not processed in accordance with the Act.

71. The mandate of this Office includes ensuring that personal data is processed in accordance with the right to privacy. It was therefore important for this Office to obtain copies of these investigation reports so as to establish the nature and scope of the processing of any personal data contained therein and whether the same was done in accordance with the right to privacy, particularly the principles of data protection and the rights of the data subject.

72. In the exercise of its powers under Section 9(1)(e) of the Act and its investigative mandate in Section 57 (1)(b) of the Act, the Office formally requested the production of the investigation reports from Scangroup and WPP to facilitate its investigation into the complaint, *vide* letters dated 27th September, 2024.

73. In a letter dated 4th October, 2024, Scangroup and WPP stated as follows in summary –

- The subject matter of the Suit is centred around the findings of the investigation report and that the same is confidential and privileged.
- The processing of the Complainant's personal data during investigations was in accordance with the Act, the WPP Data Privacy and Security Charter and the Complainant's Service Contract.
- The investigations were carried out on devices owned by Scangroup and in line with the data protection principles.
- The access given to CMA was limited in nature and at all times in Scangroup's control.

74. Scangroup and WPP maintained that the investigation report is confidential and legally privileged pending determination of the Suit. The Scangroup Head of Legal in his written statement reiterated as follows –

> *The ODPC investigating team has asked for these documents again on 14th October 2024, but we have maintained our position for not being able to share as stated above in view of the Suit.*

75. Scangroup and WPP wilfully failed, refused or neglected to produce the investigation reports and comply with this lawful request. On account of their non-cooperation, this Office was unable to establish the nature of personal data processed during the investigations by CRG and whether the personal data was processed in compliance with the Act.

76. Separately, the Office requested for the same investigation report from the CMA. In their response dated 2nd October, 2024, the CMA stated, *inter alia*, that they are unable to share the report due to the legal restriction contained in Section 13(2) of the Capital Markets Act which prohibits the CMA from disclosing any return or information acquired through their regulatory powers unless required to do so by a court of law.

77. Additionally, in a letter dated 1st October, 2024, CRG was requested for a copy of the Agreement entered into between themselves and Coulson Harney LLP on behalf of Scangroup and the Agreement entered into between themselves and WPP, the basis upon which the investigation was undertaken.

78. CRG responded in a letter dated 8th October, 2024 attaching a redacted copy of a Proposal for investigation support document dated 19th February, 2021, executed by representatives of WPP 2005 Limited, Control Risks Group Limited and Coulson Harney LLP. The same is marked 'privileged and strictly confidential'.

G. ISSUES FOR DETERMINATION

79. Having considered the nature of the complaint, the evidence adduced by all parties to the complaint and the investigations conducted by this Office, the issues for determination are therefore:

i. Whether this Office has jurisdiction to determine the complaint;

ii. Whether there was infringement of the Complainant's rights under the Act;

iii. Whether the Respondents fulfilled their obligations under the Act; and

iv. Whether the Complainant is entitled to the remedies sought.

80. **The Office wishes to state from the onset that** we shall refrain from interrogating the allegations on [redacted] which are outside our mandate under the Act, and restrict ourselves to the question of whether there was a violation of the Complainant's right to privacy under Article 31(c)&(d) of the Constitution and the Data Protection Act.

I. WHETHER THIS OFFICE HAS JURISDICTION TO DETERMINE THE COMPLAINT.

81. The Respondents informed this Office of the existence of a suit filed by the Complainant at the High Court of Kenya, Commercial division, being *HCCOMM/E147/2024 – Bharat Kumar Thakrar Vs WPP Plc, WPP Scangroup Plc & 7 Others* ('the Suit').

82. According to the Respondents, the aforementioned suit would seriously prejudice them and have a detrimental impact on the outcome of the litigation. They requested that the investigation of the Complaint by this Office be suspended or alternatively dismissed pending the outcome of the Suit in view of the *sub judice* rule as the matters pending before court inevitably touch on issues currently before this Office for determination.

83. *Sub judice* is a jurisdictional challenge as it excludes this Office from hearing and determining matters which raise substantially similar issues raised in other matters already filed and subsisting before Court. It is for this reason that this Office will make a determination on this matter at the outset.

84. For this Complaint to be found to be *sub judice*, this Office must satisfy itself that the issues raised in the Complaint are directly and substantially similar to those raised in the Suit, proceeding between the same parties and that this Office has jurisdiction to grant the reliefs claimed in the Suit.

85. The Respondents maintain that in paragraph 31 of the Plaint, the Complainant references his request to be furnished with a copy of a report containing the investigation of allegations against him and this assertion is identical to what is being sought by the Complainant from this Office. They aver that there is an overlap between the claims in the Suit and the requests in the DSARs and that

the subject matter of the suit is directly relevant to the DSAR in view of the information requested.

86. The Complainant takes the position that there are no claims or prayers for relief relating to the breach of the Act in the Plaint, most specifically:-
    i. the denial of the Complainant's data subject rights;
    ii. unauthorized access to the Complainant's personal data;
    iii. processing of personal sensitive data without consent;
    iv. unauthorized processing activities subjected to the Complainant's personal data;
    v. breach of the principles of data processing.
87. Having reviewed the Complainant's Plaint, and the 1st and 2nd Respondent's statements of defence, this Office finds that the Complainant's causes of action in the Suit include –
    - WPP's alleged interference with the contractual relations between the Complainant and Scangroup.
    - Alleged unlawful inducement of breach of contract in respect of the Complainant's contract with Scangroup.
    - Alleged breach by Scangroup & WPP of their duty of care not to act in such manner as would cause the Plaintiff financial loss, loss of reputation and invasion of privacy in his capacity as a founder shareholder, director and CEO of the 2nd Defendant.
    - Alleged conspiracy by Scangroup & WPP to injure the Plaintiff in his status and reputation as a founder shareholder, director and CEO of the 2nd Respondent.
    - Alleged discrimination of the Complainant by WPP.
88. Paragraph 31 of the Plaint which Scangroup and WPP highlight, states as follows –

> *The Plaintiff avers that the 2nd Defendant denied his request to be furnished with the report containing the allegations against him, and which formed the basis for his suspension.*

89. From this Office's reading of paragraph 31 of the Plaint, the Complainant brings to the Court's attention the fact that Scangroup denied his request to be furnished with the report containing the allegations against him. Paragraph 31 does not call the Court to make any finding as to whether there is a violation of the right of access provided for under Section 26(b) of the Act.

90. As stated hereinbefore, this Office 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.

91. The functions of this Office include to oversee the implementation of and be responsible for the enforcement of the Act and to investigate any complaint by any person on alleged infringements of the rights under the Act as set out in Sections 8 (a)&(f) of the Act.

92. This Office has no mandate to consider the issues raised in the Suit which are centred around the contractual and commercial relationships between the Complainant and the Defendants in the suit. The causes of action in the Suit and the Complaint are significantly different.

93. A review of the grounds for the complaints against the Respondents as well as the remedies sought by the Complainant as set out hereinbefore in this determination clearly demonstrates that the same are properly for consideration before this Office. It is this Office that is mandated to consider matters concerning the right to privacy under Article 31 (c)&(d) and any actions or inactions under the Data Protection Act, 2019.

94. Additionally, the 3rd Respondent herein, CRG is not a party to the Suit. Further, the persons named as the 3rd – 9th Defendants in the Suit, are not a party to this Complaint. The Complaint and the Suit cannot therefore be said to be between the same parties.

95. Further, the remedies sought in the Plaint are not within the realm of remedies envisaged under the Act and Regulations thereto, and in particular Regulation 14 (3) of the Enforcement Regulations. There is no likelihood that this Office may make similar or different findings on the same rights claimed by the parties or that there would be a duplication or a conflict of the remedies.

96. In that regard, this Office finds that as far as **Issue I** is concerned this Complaint is not *sub judice* the Suit. The Office has the requisite jurisdiction to investigate and determine the complaint.

II. WHETHER THERE WAS INFRINGEMENT OF THE COMPLAINANT'S RIGHTS UNDER THE ACT

97. Section 26(b) of the Act provides that a data subject has the right to access their personal data in custody of data controller or data processor.

98. It is not in dispute that the Complainant submitted DSARs dated 25th & 26th April, 2024 to WPP and Scangroup respectively. Scangroup and WPP responded to the DSAR on 3rd May, 2024.

99. The Complainant was dissatisfied with the responses to the DSARs. On the other hand, the Respondents maintained that the DSARs were a fishing expedition, broad, manifestly excessive and that the information requested therein was protected by legal privilege and confidentiality.

100. For context, it is important to set out the law as far as data subject access rights are concerned. Regulation 9 of the General Regulations provides as follows –

> *(1) A data subject has a right to obtain from the data controller or data processor confirmation as to whether or not personal data concerning them is being processed, and, where that is the case, access to the personal data and the information as to—*
>
> *(a) the purposes of the processing;*
>
> *(b) the categories of personal data concerned;*
>
> *(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, including recipients in other countries or territories;*

(d) where possible, the envisaged period for which the personal data may be stored, or, if not possible, the criteria used to determine that period; and

(e) where the personal data is not collected from the data subject, any available information as to the source of collection.

(2) A data subject may request to access their personal data in Form DPG 2 set out in the First Schedule.

(3) A data controller or data processor shall—

(a) on request, provide access to a data subject of their personal data in its possession;

(b) put in place mechanisms to enable a data subject to proactively access or examine their personal data; or

(c) provide the data subject with a copy of their personal data.

(4) A data controller or a data processor shall comply with a request by a data subject to access their personal data within seven days of the of the request.

(5) Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

(6) Compliance with a request for access to personal data shall be free of charge.

101. In their responses to the DSARs, the Respondents either took the position that the information sought was exempt on the basis that it was legally privileged, exempt from the application of the Act, that the request was too broad/vague or that the DSARs fell outside the scope of Section 26. The Office will therefore address itself to the following questions –

i. Are there exemptions to the exercise of the right of access under the Act?
ii. What was the nature and scope of the DSAR?

i. Are there exemptions to the exercise of the right of access under the Act?

Legal privilege

102. The Respondents stated that the DSARs are a "fishing expedition" to circumvent the proper discovery process in the ongoing Suit which was initiated by the Complainant.

103. According to them, this information is protected by legal privilege and can be requested through a disclosure request in the course of the ongoing suit between the Complainant and the 1st & 2nd Respondents.

104. The 1st & 2nd Respondents posited that they are under no legal obligation to provide explanations as to why certain information/documents are protected by legal privilege and attendant confidentiality when these are rights that automatically arise with respect to information/documents exchanged between them and their professional advisors.

105. Further, they state that it is challenging and nearly impractical for them to provide explanations to the Complainant regarding the nature of information requested that are covered by legal privilege without jeopardising the legal privilege covering such information.

106. CRG took the position that as their engagement for the investigation was with Coulson Harney LLP, acting as legal advisors to Scangroup, all investigative data, communications and reports specifically requested by the Complainant on the investigation are subject to legal privilege and confidentiality. Their engagement was for the "provision of confidential and privileged legal advice" and that the investigative data and report provided to Coulson Harney LLP informed the legally privileged advice it gave to Scangroup on matters directly in issue in the Suit and is thus protected by legal privilege.

107. Legal Privilege is provided for in Sections 134 to 137 of the Evidence Act. Section 134 of the Evidence Act provides that no advocate shall at any time be permitted unless with his client's express consent, to disclose any communication made to

him in the course and for the purpose of his employment as such advocate, by or on behalf of his client, or to state the contents or condition of any document with which he has become acquainted in the course and for the purpose of his professional employment, or to disclose any advice given by him to his client in the course and for the purpose of such employment.

108. In summary, legal privilege protects confidential communications and confidential documents between a lawyer and a client made for the purpose of the lawyer providing legal advice or professional legal services to the client, or for use in current or anticipated litigation.

109. Unlike the Access to Information Act, No. 31 of 2016 which at Section 6 (1)(i) limits the right of access to information under Article 35 of the Constitution in respect of information whose disclosure is likely to infringe professional confidentiality as recognized in law or by the rules of a registered association of a profession, the Data Protection Act, No. 24 of 2019 does not contain any such limitation.

110. The right of access under the Act is not stymied if the personal data in question consists of information in respect of which a duty of confidentiality is owed by a professional legal adviser to a client of the advisor.

111. Nonetheless, in appreciation of the sanctity of the common law principle of legal privilege, this Office finds that there are no competing duties on the Respondents between the duty to maintain legal privilege and the duty to give effect to the right of access to personal data.

112. Where there is what may be perceived as an overlap between legal privilege and the right of access to personal data, the data controller or data processor ought to develop mechanisms to give effect to the right of access while maintaining legal privilege.

113. The Respondents could have redacted any confidential and/or legally privileged information without affecting the Complainant's personal data and his right to access as provided for in Regulation 9 of the General Regulations.

General Exemption

114. In their responses to some of the Complainant's DSARs, the Respondents stated that they were exempt from fulfilling the DSARs pursuant to the general exemptions in Section 51 of the Act. Specifically, they rely on the grounds of public interest and in particular, that there was a permitted general situation under Regulation 56 of the General Regulations.

115. Section 51(2)(b) of the Act provides that the processing of personal data is exempt from the provisions of the Act if it is necessary for national security or public interest.

116. Regulation 55(a) of the General Regulations provides that for the purposes of Section 51(2) (b) of the Act, the processing of personal data is exempted from the Act on the grounds of public interest where such processing exists as a permitted general situation.

117. Permitted general situations are set out in Regulation 56 of the General Regulations and relates to the collection, use or disclosure by a data controller or data processor of personal data about data subject including for—

(a) lessening or preventing a serious threat to the life, health or safety of any data subject, or to public health or safety;
(b) taking appropriate action in relation to suspected unlawful activity or serious misconduct;
(c) locating a person reported as missing;
(d) asserting a legal or equitable claim;
(e) conducting an alternative dispute resolution process; or
(f) performing diplomatic or consular duties.

118. It is undisputed that Scangroup is a publicly listed company, regulated under the Capital Markets Act. Scangroup, through Coulson Harney LLP instructed CRG to conduct investigations on the Complainant. Upon conclusion of the investigations, the investigation report was shared with CMA in line with Section 13 (1) of the Capital Markets Act to evaluate whether regulatory breaches had

occurred at Scangroup as the Complainant was the CEO & Director of a publicly listed company.

119. The public interest exemption under the permitted general situation outlined in Regulation 56 (b) of the General Regulations would have applied for investigations carried out to facilitate compliance with the regulatory compliance requirements under the Capital Markets Act.

120. **However**, Section 51(1) of the Act is instructive in that nothing in the exemptions to the Act shall exempt any data controller or data processor from complying with data protection principles relating to **lawful processing**, **minimisation of collection**, **data quality**, and **adopting security safeguards to protect personal data**.

121. Therefore, while the public interest exemption may apply in instances of investigations in compliance with regulatory action, this Office must consider whether such processing complied with Section 51(1) of the Act.

122. The general exemptions are not blanket exemptions and must be interrogated as against Section 51(1) of the Act.

Vague, broad, costly and manifestly excessive DSAR

123. Section 26(b) of the Act as read with Regulation 9 of the General Regulations are instructive as to the scope and nature of the right of access. Other than the Exemptions set out in Part VII of the Act, there are no other exemptions or limitations to the right of access.

124. As to cost, Regulation 9(6) of the General Regulations are instructive to the effect that compliance with a request for access to personal data shall be free of charge.

ii. What was the nature and scope of the DSAR?

125. The scope of the right of access to personal data is set out under Section 26 (b) as read with Regulation 9 of the General Regulations. The right of access is the right to obtain from the data controller or data processor confirmation as to –

- Whether or not personal data concerning them is being processed, and
- Where their personal data is confirmed to be processed, access to the personal data and the information as to—

  (a) the purposes of the processing;

  (b) the categories of personal data concerned;

  (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, including recipients in other countries or territories;

  (d) where possible, the envisaged period for which the personal data may be stored, or, if not possible, the criteria used to determine that period; and

  (e) where the personal data is not collected from the data subject, any available information as to the source of collection.

126. This Office has perused the DSAR Forms DPG2 submitted to the Respondents by the Complainant. While the requests were extensive, the Office has categorized the DSARs to the following broad categories of documents and information –

<u>Policies and internal agreements and procedures</u>

- The 1st & 2nd Respondents' policies that governed the handling, protection and use of personal data within Scangroup during the Complainant's tenure, audit reports of the said policies and evidence of their active implementation.
- Documentation of consent regarding the use of his personal data and notifications governing the use of company provided devices.
- Scope of data processing arrangement between Scangroup and WPP and documentation authorising WPP's processing of his personal data, as well as the nature of processing relationship between CRG and Scangroup.
- All board collaboration documents.

- Details of data sharing and third party disclosures, the specific data shared, the dates they were shared and with whom and explanations of the purposes and legal bases for the sharing.

Data related to employment

- His employment data including his signed employment contract and all personal data held about him for the period of his employment from 5th December, 2005 to 23rd March, 2021, including board meetings where his employment was discussed.
- A detailed account of the data processing and legal bases including the processing of his personal data during employment any information relating to any automated decision making processes in relation to his employment.
- General access to all non privileged correspondences and communications between WPP, CRG and their other processors regarding his employment, position on the board.
- The 1st & 2nd Respondent's Human Resource Policy in force for the period beginning January 2005 until March 2021 specifying how his personal data would be handled during the period of his employment.
- Copies of all non-privileged correspondences, meeting notes and interactions between WPP Officers where his personal data was processed, including consents, categories of personal data processed and the purpose of processing.

Data related to the investigations

- All documents related to any investigations involving him, all communications related to the investigations, the complete and final investigation report, the investigation report forwarded to CMA, all records of board meetings where his investigation was discussed.
- Data points and procedures used by the Respondents to collect and analyse WhatsApp texts from his mobile phone and laptop to determine the handling of his personal data. This included details of access, logs, legal

bases, data extraction activities all personal data extracted from his mobile phone, WhatsApp messages and laptop.

- A detailed account of the data processing and legal bases including the processing of his personal data through the investigations and any information relating to any automated decision making processes in relation to the investigation.
- Data collected through the whistleblowing channels.
- Communications involving external parties during the period of his employment, including communications with external law firms, CRG & WPP related to their role in the investigations or decisions about his employment.
- Copies of communications related to the IT infrastructure used for conducting investigations.
- General access to all non privileged correspondences and communications between WPP, CRG and their other processors regarding the investigations.
- All personal data collected about him during the cyber security investigation related to his employment at Scangroup.

127. In this context, and upon a review of the information requested in the DSARs as summarised hereinbefore, the Office makes the following findings –

- The DSARs in respect of **policies, internal agreements and procedures (Nos. (i) – (v))** are outside the scope of the right of access under Section 26(b) of the Act as read with Regulation 9 of the Enforcement Regulations. The nature and scope of these requests relate to the right to information under the Access to Information Act.
- The DSARs in respect of **personal data related to his employment (Nos. (vi) – (x))** relates to the right of access and as such falls within the scope of Section 26(b) of the Act as read with Regulation 9 of the Enforcement Regulations only to the extent of processing in respect of his employment data. The Respondents were obligated to provide the Complainant with access to all personal data related to him during the period

of his employment. In so doing, the Respondent ought to have put in place technical and organisational safeguards to protect the rights or freedoms of others and to safeguard any legally privileged and confidential information. The 1st Respondent stated that they had forwarded a soft copy of the Complainant's HR file to him on 27th August, 2024. The Complainant has acknowledged receipt thereof. The same was however forwarded outside the statutory timeline.

- The DSARs in respect of **personal data related to the investigation (Nos. (xi) – (xviii))** is exempt from the Act under the public interest exemption as stated hereinbefore in this determination, by dint of Section 51 (2)(b) of the Act as read with Regulation 56(b) of the General Regulations as the same was in the context of collection, use and disclosure of his personal data for taking appropriate action in relation to suspected unlawful activity or serious misconduct. However, this exemption is subject to an analysis of whether the processing thereof was in compliance with Section 51(1) of the Act which this Office shall consider separately in this determination.

128. In summary, as far as **Issue II** is concerned, this Office finds as follows in respect of the issue whether there was a violation of the right of access –

- The Complainant's right of access was not limited if the personal data in question consisted of information in respect of which a duty of confidentiality is owed under legal privilege. Scangroup and WPP were obligated to redact any confidential and/or legally privileged information, without affecting the Complainant's personal data and his right to access it as provided in Regulation 9 of the General Regulations.

- Other than the Exemptions set out in Part VII of the Act and the restrictions thereto, there are no other exemptions or limitations to the Complainant's right of access.

- Scangroup and WPP were under no obligation to provide the Complainant access to policies, internal agreements and procedures pursuant to a DSAR.

- Scangroup and WPP failed to give effect to the Complainant's right to access his personal data related to his employment as CEO and Director at Scangroup.

- The Complainant's right of access to personal data related to the investigations is exempt from the application of the Act in as far as those investigations were carried out to facilitate compliance with the regulatory compliance requirements under the Capital Markets Act, **subject** to Section 51 (1) of the Act.

III. WHETHER THE RESPONDENTS FULFILLED THEIR OBLIGATIONS UNDER THE ACT.

129. The 1st & 2nd Respondents are data controllers in respect of the processing in question in this Complaint, while the 3rd Respondent is sub-processor having been engaged by Coulson Harney LLP, a data processor for purposes of the investigations. The Respondents therefore have obligations pursuant to the Act.

130. Considering the grounds & legal basis for the complaint and the Respondent's responses, this Office will address itself to the following questions –

- Did the Respondents demonstrate compliance with Section 51(1) of the Act?
- Did the Respondents share the Complainant's data in accordance with the Act?
- Did the Respondents process the Complainant's sensitive personal data without his consent?

i. Did the Respondents demonstrate compliance with Section 51(1) of the Act?

131. As previously stated, the Respondents took the position that the investigations on the Complainant were exempt from the application of the Act pursuant to the general exemptions in Section 51 of the Act. Specifically, the rely on the grounds of public interest, in particular, that there was a permitted general situation under Regulation 56 of the General Regulations

132. To rely on the general exemption, the Respondent was obligated to demonstrated compliance with data protection principles relating to –

- Lawful processing;
- Minimisation of Collection;
- Data quality; and
- Adoption of security safeguards.

133. Of relevance to this Complaint is whether the Respondents demonstrated compliance with the data protection principles relating to lawful processing and minimisation of collection.

134. This Office was not presented with evidence of a data breach or a breach of the security of the Complainant's personal data.

Compliance with the principle of lawful processing

135. As far as the investigations against the Complainant are concerned, the processing of his personal data commenced sometime in late 2020 when allegations were levelled against him alleging that he had engaged in behaviour and practices amounting to gross misconduct, contrary to the terms of Scangroup's policies and procedures, its Code of Business Conduct and Board Charter.

136. The Complainant took the position that he was neither informed of the processing of his personal data during the investigations nor was there a lawful basis for the processing of his personal data during investigations.

137. Pursuant to Section 51(1) of the Act, the Respondents were enjoined to comply with the principle of lawful processing.

138. Lawful processing of personal data is set out in Section 30(1) of the Act and provides that a data controller or processor shall not process personal data unless the data subject consents to the processing for one or more specified purposes or the processing is necessary for the reasons given in subsection (b).

139. Subsection (b)provides for the following lawful basis for processing, where the processing is necessary—

(i) 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;

(ii) for compliance with any legal obligation to which the controller is subject;

(iii) in order to protect the vital interests of the data subject or another natural person;

(iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(v) the performance of any task carried out by a public authority;

(vi) for the exercise, by any person in the public interest, of any other functions of a public nature;

(vii) for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or

(viii) for the purpose of historical, statistical, journalistic, literature and art or scientific research.

140. The Respondents relied on their legitimate interest (Section 30(1)(b)(vii)) as the lawful basis for the processing of the Complainant's personal data for purposes of investigations.

141. Regulation 5(3) of the General Regulations states that the legal basis relied on under Section 30(1)(b) of the Act shall be demonstrable at all times and where a data controller uses multiple bases for different processing, the data controller shall distinguish between the legal bases being used and respond to any data subject rights requests.

142. In line with Regulation 5(3) of the General Regulations and Section 30(1)(b)(vii) of the Act, to rely on legitimate interest as a lawful basis, the Respondents was obligated to demonstrate to this Office that –

- The processing was warranted;
- The processing was conducted with due regard to the harm and prejudice to the rights and freedoms of the data subject; and
- The processing was conducted with due regard to the legitimate interests of the data subject.

143. Quite apart from reiterating that the investigation was conducted in accordance with the Data Protection Act, 2019 and the WPP Data Privacy & Security Charter, the Respondents did not provide any evidence to demonstrate compliance with Section 30(1)(b)(vii) as read with Regulation 5(3) of the General Regulations.

144. The Respondent was thus enjoined to ensure that in order to rely on legitimate interest as a lawful basis, they demonstrate to this Office that the processing was conducted with due regard to the harm and prejudice to the rights and freedoms and with due regard to the legitimate interests of the Complainant. No evidence of this was submitted by the Respondent.

145. Moreover, pursuant to Regulation 5(3) of the General Regulations, where the Respondent uses multiple bases for different processing, the data controller shall distinguish between the legal bases being used and respond to any data subject rights requests.

146. In their response to the Notification from this Office, the Respondent relied on different lawful bases upon which they processed the Complainant's personal data. This included processing necessitated for the performance of employment contract, performance necessary for compliance with legal obligations (for example, the Employment Act requires employers to keep written particulars of employment for a period of five years after the termination of employment), as well as in pursuit of the protection of their legitimate interests especially in the context of investigations into the conduct of the Complainant during the course of his employment.

147. In their responses to the DSARs, the Respondents did not respond to the data subject request specifically on the lawful basis relied upon to process the

Complainant's personal data for purposes of investigations, in violation of Regulation 5(3) of the General Regulations.

148. In addition, the Complainant had the right to be informed that the Respondents would rely on legitimate interest as the lawful basis for processing of personal data for purposes of conducting investigations. This ought to have been notified to him, prior to the processing of his personal data.

149. The Respondent did not provide this Office with any policies, specifically a data protection policy in compliance with Regulation 23 of the General Regulations, that set out the lawful purpose for processing the Complainant's personal data for purposes of investigations.

150. This Office therefore finds that the Respondents have not established a lawful basis for the processing of the Complainant's personal data for purposes of investigations.

Compliance with the principle of minimisation of collection.

151. The Respondents have an obligation under Section 25 of the Act to ensure that the Complainants' personal data is, amongst others:

(a) processed in accordance with the right to privacy of the data subject;
(b) processed lawfully, fairly and in a transparent manner in relation to any data subject;
(c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes; and
(d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed.

152. The Complainant asserts that his personal data initially collected by Scangroup for employment purposes was subsequently used by WPP & CRG for investigations without informing him or obtaining his consent. He further states that his data was shared with CMA and the usage goes beyond the original scope of data collection. This, he asserts was in violation of the principle of purpose

limitation which provides that personal data should not be further processed in a manner incompatible with the original purpose for collection.

153. On their part, the Respondents reiterate that the investigation was conducted in compliance with the Data Protection Act, 2019 and the sharing of the Complainant's personal data was pursuant to the WPP Data Privacy & Security Charter and his Service Contract.

154. As stated hereinbefore, the Complainant's personal data processed for purposes of the investigation is exempt under the public interest exemption set out in Section 51(2)(b) of the Act as read with Regulation 56(b) of the General Regulations in as far as those investigations are carried out to facilitate compliance with the regulatory compliance requirements under the Capital Markets Act, subject to Section 51(1) of the Act. The Respondents were thus exempt from complying with the principle of purpose limitation to this extent.

155. However, as earlier observed, Section 51(1) of the Act is instructive in that nothing in the exemptions to the Act shall exempt any data controller or data processor from complying with data protection principles relating to **lawful processing**, **minimisation of collection**, **data quality**, and **adopting security safeguards to protect personal data**.

156. During investigations, this Office requested both Scangroup and WPP for copies of the investigation reports forwarded to CMA. This was to ascertain whether there was compliance with Section 51(1) of the Act. Scangroup and WPP declined to provide this Office with a copy of the investigation reports forwarded to CMA.

157. Even so, this Office has reviewed the statements of both the Complainant and the 1st Respondent's legal counsel as well as the evidence on record. It is undisputed that *vide* a Notice of Suspension dated 18th February, 2021, the Complainant was suspended as CEO and director of Scangroup on various grounds including alleged [redacted].

158. Further, this Office reviewed the Notice to Show Cause dated 16th March, 2021 from the Respondent to the Complainant which made reference to the

investigations and the initial conclusions reached on the alleged misconduct of the Complainant. Clause 3.2 thereof included allegations of [redacted], established through an investigation into the Complainant's WhatsApp communications.

159. As previously stated, this Office shall refrain from interrogating the allegations on [redacted] which are outside our mandate under the Act, and restrict itself to the question of whether there was a violation of the Complainant's right to privacy under Article 31(c)&(d) of the Constitution and the Respondents' compliance with the principle of data minimisation.

160. In line with Section 51(1) of the Act and while the investigations would have been exempt under the public interest exemption, the Respondents were enjoined to comply with the principle of data minimization. The Respondents were required to ensure that the processing of the Complainant's personal data during investigations was **adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed.**

161. Neither the Notice of Suspension nor the Notice to Show Cause specified which provision of Scangroup's Human Resource Policy the Complainant had violated. This is important as it would have established the policy and/or regulatory basis upon which Scangroup investigated the Complainant's conduct so as to initiate regulatory action with CMA.

162. Moreover, Scangroup did not provide this Office the Human Resource Policy in place at the material time which they would be relying on to access the Complainant's private WhatsApp messages relating to alleged [redacted]

163. Regulation 33 of the General Regulations outline the elements necessary to implement the principle of data minimization to include—

- Limiting the amount of personal data collected to what is necessary for the purpose.
- Ability to demonstrate the relevance of the data to the processing in question.

- Anonymizing or deleting personal data where the data is no longer necessary for the purpose.
- The application of available and suitable technologies for data avoidance and minimization.

164. There is no evidence on record that the aforementioned elements were incorporated into the processing of the Complainant's personal data during investigations.

165. Moreover, the actions of the Respondents contravened Article 31 (c) & (d) of the Constitution which provides that every person has the right to privacy, which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed or the privacy of their communications infringed.

166. Article 31 (c)&(d) are the foundations upon which the Data Protection Act, 2019 is anchored. It gives a data subject the right to determine for themselves when, how, and to what extent information about them is communicated to others.

167. The Respondents failed to implement data protection by design and default so as to segregate personal data from work related data to protect the Complainant's private communication unrelated to the investigations, thereby disregarding the principle of data minimization.

168. This Office therefore finds that the Respondents failed to comply with the principle of data minimization in processing the Complainant's private WhatsApp messages relating to alleged [redacted]

169. In conclusion, the Respondents have failed to demonstrate that the processing of the Complainant's personal data during investigations complied with the data protection principles relating to lawful processing and minimisation of collection.

170. As such, having failed to comply with their obligations under Section 51(1) of the Act, the public interest exemption under Section 51 (2)(b) as read with Regulations 55(a) and 56(b) of the General Regulations does not apply to the investigations conducted by the Respondents on the Complainant.

ii. Did the Respondents share the Complainant's data in accordance with the Act?

171. The Complainant's contention in this respect was the manner in which his personal data was shared between Scangroup and WPP & Scangroup and CRG. He maintains that Scangroup and WPP did not have in place effective and compliant data handling policies at the point they violated his personal data in late 2020 and early 2021 jointly with Control Risks Group Limited (CRG) and Coulson Harney LLP.

172. In considering this question, the Office will interrogate the sharing of the Complainant's personal data pursuant to the data processing agreement, sharing pursuant to the WPP Data Privacy & Security Charter & the Service Contract and sharing of the Complainant's personal data post-employment.

Sharing pursuant to the data processing agreement

173. This Office notes that in the Proposal for Investigation Support executed by WPP, Coulson Harney LLP on instructions of Scangroup & CRG, submitted to this Office by CRG, there is contained therein a Data Protection clause and a Data Processing Agreement. This Office has reviewed the aforesaid Agreement and note that the same makes reference to the EU GDPR and matters of compliance with European Union Law and/or the national law of EU member states.

174. Section 42 (2)(b) of the Act provides that where a data controller is using the services of a data processor, the data controller and the data processor shall enter into a written contract which shall provide that the data processor shall act only on instructions received from the data controller and shall be bound by obligations of the data controller.

175. The data processing agreement was therefore compliant with Section 42(2)(b) of the Act in so far as it was a written contract that provided at page 14 that CRG shall at (a) act only on instructions received from the data controller and at (e) be bound by obligations of the data controller.

Sharing pursuant to the WPP Data Privacy & Security Charter & the Service Contract

176. It is Scangroup's and WPP's position that an extract of Clause 8 of the Complainant's Service Contract sets out how the Complainant's data was handled during the course of his employment and the WPP Data Privacy & Security Charter outline the 1st & 2nd Respondent's rights as regards data sharing. They stated that the WPP Data Privacy and Security Charter which applied at a group level on all operating entities.

177. The Complainant takes the position that the WPP Data Privacy & Security Charter does not take into account Kenya's Data Protection Act. He also takes issue with the sharing of his personal data with employees of Scangroup, without defined parameters, guidelines and safeguards. According to him, there was no evidence that the sharing was governed by either WPP and Scangroup's Shareholders Agreement or Data Protection/Privacy Policy.

178. The Office has reviewed the WPP Data Privacy & Security Charter which provides for transfer and sharing of personal data across the group's companies at Clause 5.8 and sets out the purposes and means of sharing personal data as per Regulation 21(2) of the General Regulations.

179. This Office cannot however rely on the document submitted by Scangroup and WPP purporting to be the Complainant's Service Contract as the same contains one page of an untitled document, is undated, unattributed and unsigned.

180. This Office therefore finds that the sharing of the Complainant's personal pursuant to the WPP Data Privacy & Security Charter was lawful.

Sharing of the Complainant's personal data post-employment

181. Separately, it was the Complainant's contention that Scangroup disclosed the Complainant's personal data, including details of disciplinary procedures and correspondences with WPP's legal counsel post-employment without obtaining his consent.

182. This Office notes that the WPP Data Handling and Retention Policy, places the obligation to specify data retention period on the operating companies. Scangroup and WPP stated in their response that the Kenyan Employment Act requires employers to keep written particulars of employment for a period of five years after the termination of employment.

183. The Office finds that the sharing of the Complainant's personal data post employment was lawful.

iii. Did the Respondents process the Complainant's sensitive personal data without his consent?

184. The Respondents states that no sensitive personal data of the Complainant was processed by them in the manner alleged and consequently, consent was not required. CRG asserted that as per the definition of sensitive personal data in the Act, personal conversations, WhatsApp and iCloud data is not *prima facie* sensitive personal data.

185. Sensitive personal data as defined in Section 2 of the Act means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject.

186. As previously stated, despite requesting Scangroup and WPP for copies of the investigations report, they declined to do so. The Office is therefore unable to establish whether the Complainant's sensitive personal data was processed by the Respondents so as to determine whether the same was lawfully processed in accordance with Section 51(1) of the Act.

187. In the absence of evidence, this Office cannot make a finding on whether the Complainant's sensitive personal data was processed and if the same was lawfully processed.

188. In summary, as far as **Issue III** is concerned, the Office finds as follows –

- The Respondents did not comply with the principle of lawful processing in processing the Complainant's private WhatsApp communications relating to alleged [redacted] and thus did not demonstrate compliance with Section 51(1) of the Act.
- The Respondents did not comply with the principle of data minimization in processing the Complainant's private WhatsApp messages relating to alleged [redacted] and thus did not demonstrate compliance with Section 51(1) of the Act.
- The sharing of the Complainant's personal data between Scangroup, CRG, WPP and Coulson Harney was lawful.
- There was no evidence that the Complainant's sensitive personal data was processed by the Respondents.

IV. WHETHER THE COMPLAINANT IS ENTITLED TO THE REMEDIES UNDER THE ACT

189. The Complainant sought for the following remedies against Scangroup –

(a) Immediate and full access to the personal data sought;
(b) Explanation of data processing activities;
(c) Cessation of unlawful processing and deletion of personal data;
(d) Rectification of inaccurate personal data;
(e) Restriction on further data sharing;
(f) Detailed report on data disclosures;
(g) Compensation for damages;
(h) Request for investigation and audit of Scagroup;
(i) Public notice of enforcement action;
(j) Formal apology; and
(k) Any other order or relief that the Data Commissioner may deem just and fit to grant.

190. The Complainant sought for the following remedies against WPP –

(a) A finding that WPP is in breach of his rights as a data subject and his constitutional right to privacy under Article 31 of the Constitution;
(b) Immediate and full access to the personal data sought;
(c) Explanation of data processing activities;
(d) Cessation of unlawful processing and deletion of personal data;
(e) Restriction on further data sharing;
(f) Detailed report on data disclosures;
(g) Compensation for damages;
(h) Request for investigation and audit of WPP;
(i) Public notice of enforcement action;
(j) Formal apology; and
(k) Any other order or relief that the Data Commissioner may deem just and fit to grant.

191. The Complainant sought for the following remedies against CRG –

(a) A finding that CRG is in breach of his rights as a data subject and his constitutional right to privacy under Article 31 of the Constitution;
(b) Immediate and full access to the personal data sought;
(c) Explanation of data processing activities;
(d) Cessation of unlawful processing and deletion of personal data;
(e) Restriction on further data sharing;
(f) Detailed report on data disclosures;
(g) Compensation for damages;
(h) Request for investigation and audit of CRG;
(i) Public notice of enforcement action;
(j) Formal apology; and
(k) Any other order or relief that the Data Commissioner may deem just and fit to grant.

192. In response to the prayers sought by the Complainant, Scangroup and WPP state –

(a) The allegation that they are in breach of the Complainant's rights was wholly denied;

(b) Sufficient explanations and/or reasons have been provided where requested information has not been provided to the Complainant;

(c) A comprehensive explanation of their data processing activities are contained in the WPP Data Privacy & Security Charter;

(d) Continued processing of the Complainant's personal data by them are guided by the WPP Data Handling and Retention Policy;

(e) They are available to comply with the data subject right of rectification of personal data as permitted under the DPA and to the extent that it does not prejudice the Suit or otherwise contrary to any law, upon request;

(f) The Complainant be guided by the terms of Service Contract dated 12th April 2013 and the provisions of the WPP Data Privacy & Security Charter (Annexure A) regarding the permitted instances sharing of his personal data with third parties and the safeguards in place in such instances;

(g) The Complainant has neither provided a proof for the necessity of any compensation nor a basis upon which the quoted compensation amount has been arrived at. It is furthermore wholly in excess of the statutory limits and further indicates that the DSAR was made in bad faith;

(h) They are willing to engage the Office for an inspection and audit if this Office deems it necessary;

(i) The Complainant has neither provided a basis nor proof to the effect that Scangroup has breached the provisions of the Act and thus the prayer for public notice on enforcement action is therefore not supported by any basis; and

(j) The prayer for a formal apology has no valid and lawful basis.

193. Regulation 14 (2) of the Enforcement Regulations provides that 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 as follows –

(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.

194. Whereas the Complainant has sought an array of remedies from this Office, the Office is guided by Regulation 14 (3) of the Enforcement Regulations set out above.

195. Having considered the merits of the Complaint, the evidence adduced by both the Complainant, and having found that the Respondents did not give effect to the Complainants right to access his employment data and that the Respondents failed to comply with the principles of lawfulness & data minimization, it, therefore, follows that there has been a violation of the Act by the Respondents.

196. Section 65 (1) of the Act provides for compensation to a data subject and states 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. Section 65 (4) of the Act states that "damage" includes financial loss and damage not involving financial loss, including distress.

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

198. The Complainant claimed for the remedy of compensation in the sum of KES Seven Billion Kenya Shillings (KES 7,000,000,000) against the Scangroup, Fifty Million Pounds (GBP 50,000,000) against WPP and Fifty Million Pounds (GBP 50,000,000) against CRG.

199. The Respondents stated that the Complainant has not provided proof for the necessity of any compensation nor a basis upon which the quoted compensation amount has been arrived at and that it is wholly in excess of the statutory limits.

200. The Respondents are hereby directed to jointly compensate the Complainant the amount of **KES. 1,950,000/= (One Million, Nine Hundred and Fifty Thousand Shillings Only)** for violation of the Complainant's right to access his personal data in the custody of the Respondents and for failing to comply with the principles of lawfulness and the principle of data minimization as follows–

- 1st Respondent - **KES. 700,000/= (Seven Hundred Thousand Kenya Shillings Only)**
- 2nd Respondent - **KES. 700,000/= (Seven Hundred Thousand Kenya Shillings Only)**
- 3rd Respondent - **KES.550,000/= (Five Hundred and Fifty Thousand Kenya Shillings Only)**

201. In so doing, the Office has considered the nature of the personal data processed, the severity of the violation as it relates to the actual harm or distress caused to the Complainant as a result of the violation and the impact on the Complainant's personal and professional life.

H. FINAL DETERMINATION

202. In consideration of all the facts of the complaint, the evidence tendered and the investigations conducted, the Data Commissioner makes the following determination:

i. The Respondents are found liable.

ii. The 1st and 2nd Respondents are hereby ordered to give the Complainant access to his personal data related to his employment as CEO & Director at WPP Scangroup in accordance with Section 26(b) and Regulation (9) of the Data Protection (General) Regulations, 2021 **within 7 days** of the date of this determination.

iii. The Respondents are hereby ordered to compensate the [redacted] **KES. 1,950,000/= (One Million, Nine Hundred and Fifty Thousand Shillings Only)** as follows –

- 1st Respondent - **KES. 700,000/= (Seven Hundred Thousand Kenya Shillings Only)**
- 2nd Respondent - **KES. 700,000/= (Seven Hundred Thousand Kenya Shillings Only)**
- 3rd Respondent - **KES.550,000/= (Five Hundred and Fifty Thousand Kenya Shillings Only)**

iv. An Enforcement Notice to issue to the 1st, 2nd & 3rd Respondents.

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

DATED at **NAIROBI** this 25th day of October. **2024**

IMMACULATE KASSAIT, MBS

DATA COMMISSIONER