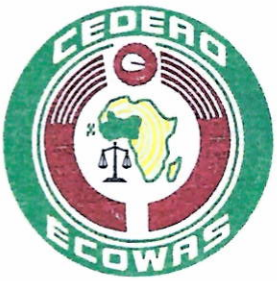
COMMUNITY COURT OF JUSTICE,
ECOWAS
COUR DE JUSTICE DE LA COMMUNATE,
CEDEAO

TRIBUNAL DE JUSTICA DA COMMUNIDADE,
CEDEAO



No. 10 DAR ES SALAAM CRESCENT
OFF AMINU KANO CRESCENT,
WUSE II, ABUJA-NIGERIA. PMB 567
GARKI, ABUJA TEL: 234-9-78 22 801
Website: www.courtecowas.org

THE COMMUNITY COURT OF JUSTICE OF THE ECONOMIC COMMUNITY OF WEST AFRICAN STATES (ECOWAS)

In the Matter of

INCORPORATED TRUSTEES OF DIGITAL RIGHTS LAWYERS INITIATIVE v. FEDERAL REPUBLIC OF NIGERIA

Application No: **ECW/CCJ/APP/37/21**; ***Judgment No. ECW/CCJ/JUD/02/23***

JUDGMENT

ABUJA

13 MARCH 2023

THE COMMUNITY COURT OF JUSTICE OF THE
ECONOMIC COMMUNITY OF WEST AFRICAN STATES (ECOWAS)
HOLDEN AT ABUJA, NIGERIA

Application No: **ECW/CCJ/APP/37/21**; ***Judgment No. ECW/CCJ/JUD/02/23***

INCORPORATED TRUSTEES OF
DIGITAL RIGHTS LAWYERS INITIATIVE — APPLICANT

AND

THE FEDERAL REPUBLIC OF NIGERIA — RESPONDENT

COMPOSITION OF THE COURT:

Hon. Justice Edward Amoako **ASANTE** - Presiding/ Judge Rapporteur
Hon. Justice Gberi-Be **OUATTARA** - Member
Hon. Justice Dupe **ATOKI** - Member

ASSISTED BY:
Dr. Athanase **ATANNON** - Deputy Chief Registrar

REPRESENTATION OF PARTIES:
Olumide **BABALOLA**, Esq.
Irene **CHUKWUKELU**, Esq. - Counsel for Applicant

Maimuna Lami **SHIRU** (Mrs.) Counsel for Respondent

I. JUDGMENT

1. This is the judgment of the Court read virtually in open court pursuant to Article 8(1) of the Practice Directions on Electronic Case Management and Virtual Court Sessions, 2020.

II. DESCRIPTION OF THE PARTIES

2. Applicant is a Non-Governmental Organisation registered under the Companies and Allied Matters Act, Laws of the Federation of Nigeria, 2004, on the 7th day of January 2019, with an office situated at Aggey House (6th Floor) 12 Berkeley Street, Off King George V, Moloney, Lagos Island, Lagos State.
3. The Applicant, a network of citizens of Nigeria comprising data protection lawyers and stakeholders, was incorporated to promote and protect citizens' digital rights, online expressions, internet-based communication, privacy and data protection.
4. Respondent is the Federal Republic of Nigeria, a Member State of the Economic Community of West African States, ECOWAS and a signatory to the Supplementary Act A/Sa 1/01/10 on Personal Data Protection Within ECOWAS.

III. INTRODUCTION

Subject matter of the proceedings

5. Applicant alleges that the Respondent has consistently violated its international obligations by failing to enact comprehensive legislation and legal framework on data protection in contravention of the provisions of the Supplementary Act A/Sa.1/01/10 on Personal Data Protection within ECOWAS.

III. PROCEDURE BEFORE THE COURT

6. The Originating Application dated 19 July 2021 was filed at the registry of the Court and served on the Respondent electronically the same day.

7. Respondent filed a Motion for Extension of Time to file Statement of Defence together with the Statement of Defence, Plea in Law/Statement of Facts in opposition to the Applicant's Application, all dated 20 December 2021 on 5 December 2022 were served electronically on the Applicant the same day.

8. On 6 December 2022, a virtual court session was held where the Applicant was represented in Court, but the Respondent was absent without any representation. The Respondent's motion for an extension of time was granted, and its statement of defence was adopted. The case was heard on the merits. The applicant adumbrated and adopted its written submissions as its argument in the case and was adjourned for judgment.

IV. APPLICANT'S CASE

a. Summary of facts

9. Applicant claims that on 16 February 2010, the Authority of Heads of State and Government of the Economic Community of West African States (ECOWAS), during its thirty-seventh session, adopted a regional legal framework for personal data protection within ECOWAS, i.e. *SUPPLEMENTARY ACT A/SA.1/01/10 ON PERSONAL DATA PROTECTION* (hereinafter referred to as *"the Supplementary Act"*.

10. The Applicant added that the intendment of the Supplementary Act is to impose obligations on Member States of ECOWAS to establish

comprehensive national data protection laws that will meet up with the challenges caused by the internet, which increasingly raises the problems of data protection notwithstanding the existence of national legislations of Member States relating to the protection of privacy of their citizens in their private and professional life.

11. The Applicant further contends that by signing the Supplementary Act, each Member State agreed to comply with the provisions of the said Act by enacting a comprehensive legal framework on personal data protection for their respective States, including the Respondent.
12. The crux of the Applicant's claims is that the Respondent, as a signatory to the Supplementary Act, has a mandatory obligation to enact comprehensive legislation on data protection to protect its citizens' rights to data privacy, but the latter has consistently failed to do so in contravention of its duty under international conventions and treaties ratified by her.
13. The failure of the Respondent to enact comprehensive legislation on data privacy, according to the Applicant, has interfered with its right to data privacy and thus constitutes a breach of the former's obligations imposed by the Supplementary Act in particular and generally under other binding international instruments explicitly delineated in the Applicant's pleas in law session of this judgment.

b. Pleas in Law

14. Applicant pleads and relies on the following laws:
    a. Articles 1, 2, 3, 4, 5, 6, 7, 8, 9,10,11,12,13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 30, 31, 32, 33, 34, 35, 36, 37, 45 & 48 of the

Supplementary Act A/Sa 1/01/10 on Personal Data Protection within ECOWAS, and

b. Article 17 of the International Covenant on Civil and Political Rights (ICCPR)

c. Reliefs Sought by the Applicant

15. For the reasons above, the Applicant is seeking the following from the Court;

*1) **A DECLARATION** that the Defendant's non-compliance with its international obligation under the Supplementary Act A/Sa 1/01/10 on Personal Data Protection Within ECOWAS by enacting a comprehensive framework on data protection interferes with the right to data privacy of the Applicant.*

*2) **AN ORDER** of the ECOWAS Court compelling the Federal Republic of Nigeria to pass a comprehensive framework on data protection.*

*3) **CONSEQUENTIAL ORDER(S)** as this honourable court may deem fit to make in the circumstance.*

V. RESPONDENT'S CASE

a. Summary of facts

16. Respondent denies the Applicant's claim and states that it has not failed to enact a comprehensive legislation and legal framework on personal data protection in compliance with its duty under International Conventions and treaties it has ratified.

17. The Respondent explicitly denies any violation of the provisions of the Supplementary Act cited by the Applicant and Article 17 of the ICCPR and contends that it has instead promulgated several laws serving as the

bulwark against any potential breaches of its citizens' right to personal data protection.

18. Respondent submitted that the crux of this matter relates to an alleged failure of the Respondent to honour its obligation by enacting legislation on data privacy under the Supplementary Act. This fact renders the Application incompetent since only Member States can seek relief to enforce their obligation under the Supplementary Act.
19. It is further contended by the Respondent that the Applicant's suit is an invitation to the Court to interfere with municipal laws of the Member State for which the Applicant has no locus.
20. The Respondent states that the Applicant has not disclosed any actionable wrong done to it by the Respondent that would warrant the court granting the orders sought by it.

b. Pleas in Law

21. By way of pleas in law, Respondent pleaded the following legislations in support of its case:
    a. Section 12 & 37 of the 1999 Constitution of the Federal Republic of Nigeria (as amended;
    b. Nigeria Data Protection Regulation (NDPR) 2019;
    c. Section 6 of the National Information Technology Development Agency (NITDA) Act (2007);
    d. The Nigerian Communications Commission (NCC) Consumer Code of Practice Regulation 2007 Federal Republic of Nigeria Official Gazette NO. 87 10th July vol.94;
    e. The Nigerian Communications Commission (NCC) Registration of Telephone Subscribers Regulation 2011;
    f. The Freedom of Information Act 2011;

g. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015;

h. The Child Rights Act 2003;

i. The Consumer Protection Framework 2016;

j. The National Identity Management Commission (NIMC) Act 2007;

k. The National Health Act (NHA) 2014;

l. The Federal Competition and Consumer Protection Act 2019;

m. The Nigerian Data Protection Regulation 2019; and

n. Articles 3 & 5 of the Revised Treaty of the Economic Community of West African States (ECOWAS)

c. Reliefs sought

22. The Respondent urges the Court to dismiss the Applicant's case on the grounds that the same is frivolous, speculative, vexatious, baseless and incompetent.

VII. JURISDICTION

23. Article 9(4) of the Supplementary Protocol (A/SP.1/01/05) amending the Protocol (A/P1/7/91) on the Court provides thus:

"The Court has jurisdiction to determine cases of violation of human rights that occur in any Member State."

24. The Court's jurisdiction to entertain and determine suits regarding the violation of fundamental rights of a citizen of a Member State of ECOWAS has been settled in a plethora of cases, among which is *BAKARE SARRE & 28 ORS v. THE REPUBLIC OF MALI (2011) CCJELR 57*, where the Court stressed that: "*Once human rights violation which involves international or community obligations of a Member State is alleged, it will exercise its jurisdiction over the case.*

25. In light of the above, it is incumbent on the Court in its examination of its subject matter jurisdiction to consider whether the instruments on which Applicant relies for its claims are human rights instruments under which the Respondents has undertaken human rights obligations. In this case, Applicant primarily relies on the Supplementary Act A/SA 1/01/10 on Personal Data Protection within ECOWAS. Therefore, the Court must satisfy itself that the Supplementary Act is a human rights instrument whose human rights obligations the Respondent has allegedly violated. Confronted with a similar issue regarding the African Charter on Democracy and the ECOWAS Protocol on Democracy, the African Court noted that it had to 'satisfy itself that these two instruments namely, the African Charter on Democracy and the [ECOWAS] Democracy Protocol are human rights instruments. (See *ACTION POUR LA PROTECTION DE DROITS DE L'HOMME (APDH) v COTE D'IVOIRE*, Application No. 001/2014, para 49).

26. A similar analysis is required here. In the *APDH v Cote d'Ivoire* case, the African Court held that in determining whether a treaty is a human rights instrument, it is important to consider the purpose of the instrument as reflected in 'an express enunciation of the subjective rights of individuals or groups of individuals, or by mandatory obligations on state parties for the consequent enjoyment of the said rights.' (*ACTION POUR LA PROTECTION DE DROITS DE L'HOMME (APDH) v COTE D'IVOIRE*, Application No. 001/2014, para 57).

27. Regarding express enunciation of subjective rights of individuals, Articles 38 to 41 of the ECOWAS Supplementary Act on Data Protection 2010

guarantees certain rights of individuals as far as the processing of their private information is concerned. These are

(i) the right of individuals to be informed about the data that is being collected about them including the purpose of the data collection, their right to request rectification of the data and whether the data may be transferred to a third party or country (Article 38);

(ii) an individual's right of access to the data collected including requesting information about the categories of data being processed about him or her and whether the data will be disclosed to third parties (Article 39);

(iii) an individual's right to object to data that is being processed about him or her (Article 40); and

(iv) the right of an individual to request for the rectification or destruction of the data collected if the data is, among others, inaccurate, questionable, outdated, or incomplete (Article 41).

28. In terms of the state parties' obligations, Article 2 of the Supplementary Act requires that each state 'shall establish a legal framework for protection of privacy of data relating to the collection, processing, transmission, storage, and use of personal data without prejudice to the general interest of the state'. This is additional to other more specific obligations such as the duty of member states to establish independent data protection Agencies to ensure that collection and processing of personal data is compliant with the provisions of the Supplementary Act.

29. From the express guarantee of personal rights of individuals under the Supplementary Act and the obligations of member states to ensure the protection of those rights, it can be concluded that the ECOWAS Supplementary Act on Data Protection is a human rights instrument with the object of securing the privacy rights of individuals to their personal information. In this regard, it is also significant that one of the objectives of the Supplementary Act is to effectuate the obligation of member states under Article 4(g) of the ECOWAS Revised Treaty to promote and protect human rights consistent with the African Charter on Human and Peoples' Rights. (*Preamble of the Supplementary Act*). In this context, the Supplementary Act can be seen as complementing and reinforcing the protection of certain internationally recognised human rights, especially, the right to privacy guaranteed under Article 17 of the International Covenant on Civil and Political Rights 1966 and the right to information guaranteed in Article 9 of the African Charter.

30. Accordingly, since the Applicant's case alleges violations of the provisions of instruments that guarantee human rights, especially, the right to privacy of personal data, the suit falls within the human rights jurisdiction of the Court.

VIII. ADMISSIBILITY

31. The Applicant, registered as Non-Governmental Organisation (NGO) comprising data protection lawyers and their stakeholders, claims a violation of the right to personal data protection of its members due to the failure of the Respondent to enact a comprehensive legal framework on data protection. They can, therefore, be considered as victims of

alleged human rights violation within the meaning of Article 10(d) of the Court's Protocol. Besides, since the application is not anonymous and has not been filed before another competent international Court, the admissibility criteria provided by Article 10 (d) of the Protocol on the Court as amended are satisfied. (See the case of **ASSIMA KOKOU INNOCENT & ORS v. REPUBLIC OF TOGO (2013) CCJLER pg. 197).**

32. The Application, having been held to be in compliance with the Court's rules of admissibility, is hereby admitted for determination on the merits in consideration of the parties' submissions and arguments and the Court so holds.

IX. MERITS

33. The Applicant's claim of violation of the rights of its members and stakeholders hinges on the following headings, which shall be determined in seriatim:

i. Allegation of violation of the right to privacy by the Respondent for failure to enact a comprehensive framework on personal data protection;

ii. Allegation of breach of the Respondent's international obligations under the Supplementary Act of ECOWAS; and

iii. The issue of compellability of the Respondent to pass a comprehensive framework on data protection.

34. Contrary to the claim of violation of their right to data protection, the Respondent submits that the Applicant has not disclosed any actionable wrong done to it by the Respondent, warranting the court granting the

orders sought by it. The Court notes that every alleged human rights violation must be proved with concrete evidence by whosoever alleges. In *HEMBADOON CHIA & 7 ORS v. FEDERAL REPUBLIC OF NIGERIA & ANOR (ECW/CCJ/JUD/21/18) @ pg. 27 (Unreported),* the Court maintained that it "*has repeatedly stated that it will not act on a mere allegation of violation, but each allegation must be substantiated with some concrete facts as the case may require*".

35. The burden of proving every allegation of violation of human rights rests on the party who alleges, and until he or she does that, the burden stays the same. See the case of *FESTUS A.O. OGWUCHE v. FEDERAL REPUBLIC OF NIGERIA ECW/CCJ/JUD/02/18 @ pg. 33 (Unreported),* in which the Court stated that *"as a general rule, the burden of proof lies on the Applicant. If that burden is met, the burden then shifts to the Respondent, who now has to plead and prove any defence by a preponderance of evidence''.*

36. It is against these time-tested principles of proof, well imbued in the Court's jurisprudence, that the allegations of infringement of the rights of the members of the Applicant's NGO shall be evaluated and determined as set forth under paragraph 29 *supra.*

a. ***Allegation of violation of the right to privacy by the Respondent for failure to enact a comprehensive framework on personal data protection***

37. The Court observes from the pleadings of the parties that they are agreeable on the adoption of the *SUPPLEMENTARY ACT A/SA.1/01/10*

ON PERSONAL DATA PROTECTION by the ECOWAS Member States of which the Respondent is a member. The Court further notes that the Respondent has not explicitly promulgated any legislative framework in direct response to the Supplementary Act per se but has in place several legislations (some that predated and others that postdate the adoption of the Supplementary Act) addressing the import of the Supplementary Act.

38. It is the Respondent's failure to promulgate a specific law in direct response to the Supplementary Act that the applicant claims have infringed on the right of its members and stakeholders to privacy. On the authority of *HEMBADOON CHIA & 7 ORS v. FEDERAL REPUBLIC OF NIGERIA & ANOR (supra),* such a determination can only be made on the back of factual demonstrations of the extent of the infringement. The applicant has produced no evidence regarding the nature of the breach of the right to privacy or the extent of such violation.

39. Rather, the Applicant has surmised and invited the Court to assume that the absence of a 'comprehensive legal framework on data protection' automatically interferes with the right to privacy. However, the Court notes that human rights actions are personal causes of action. The jurisprudence of the Court clearly demands that a person who alleges violation of a right must factually demonstrate actual damage/harm suffered or being suffered on account of the Member State concerned. Failing this, the court cannot *suo motu* assume damage or injury from the absence of a set of circumstances. Indeed, Respondent rightly notes in paragraph 1.23 of its submission that Applicant has produced no element of fact in proof of its allegation of violation of human rights.

40. For the above reason, the Court is unable to agree with the Applicant that the '*non-compliance with its international obligation under the*

Supplementary Act A/Sa 1/01/10 on Personal Data Protection Within ECOWAS by enacting a comprehensive framework on data protection interferes with the right to data privacy of the Applicant'. Consequently, the Applicant's claim under this heading fails, and the same is dismissed.

b. ***Allegation of breach of the Respondent's international obligations under the Supplementary Act of ECOWAS***

41. The Applicant further contends that by the combined effect of Articles 2 and 14 of the Supplementary Act, the Respondent is in breach of its obligations to establish a comprehensive legal framework for data protection under the Supplementary Act. The Respondent denies any violation of its international obligation as alleged.

42. From the very outset, the Court observes that the Supplementary Act does not use the word "comprehensive" throughout the Act. This is a creation of the Applicant, perhaps, with a certain image of how the framework required under the Act ought to be. Article 2 only requires the establishment of a legal framework of protection for the privacy of data relating to the collection, processing, transmission, storage, and use of personal data without prejudice to the general interest of the State.

43. Respondent has listed a host of legislations containing provisions geared towards meeting the objectives of the Supplementary Act. Admittedly, several of these legislations predate the Supplementary Act and - Child Right Act, Consumer Protection Framework, Federal Competition and Consumer Protection Framework, and Cybercrimes (Prohibition and Prevention). - are sectoral and hence narrow in their application despite containing provisions on protecting privacy and disclosure of personal data/information under these legislations.

44. The Court equally takes judicial notice of other sectoral laws of the Respondent, such as the Credit Reporting Act, which contains provisions on the retention, protection and disclosure of credit information (personal data) in Sections 5 and 9, respectively. Significantly, the most fatal blow dealt to the Applicant's case of the absence of a framework is the Nigeria Data Protection Regulation 2019 (NDPR) and its implementation framework of 2020, although not mentioned by the Respondent.

45. The NDPR subsidiary legislation contains provisions covering conditions for processing, controllers' obligation, data subject rights, enforcement mechanisms, redress panels and cross-border transfers. The Implementation Framework, whose relationship to the Regulation is noted under paragraph 2 as clarifying provisions of the NDPR and thus must be read in conjunction with the NDPR, provides a detailed explanation of the various requirements of the NDPR.

46. The Court observes that some of the obligations under the NDPR, such as the designation of data protection officers under 4.1 (2), are not even provided for under the Supplementary Act. Consequently, it is inaccurate for the Applicant to contend that there is no legal framework for protecting privacy or personal data. The Court finds that, although a substantive Act of Parliament may yet set up such a framework, the NDPR and its implementation framework equally constitute a framework within the meaning of the Supplementary Act.

47. The NDPR and its framework at the time this action was initiated was administered by the National Information Technology Development Agency (NITDA), which is empowered to fine offending data controllers to the tune of 2% or 1% annual gross revenue depending on its number of data subjects.

48. NITDA is charged with ensuring compliance with the NDPR. This mandate appears to be Applicant's quandary; because while Applicant does not challenge the provisions of the NDPR and its framework or its capacity to meet the terms of the Supplementary Act, they contend strongly that NITDA lacks the independence required of a Data Protection Authority under Article 14 of the Supplementary Act.

49. Regrettably, the Applicant fails again to provide any evidence of the composition of NITDA or why it lacks the independence required under the law. As stated earlier in this judgment, the Applicant has left the Court to assume that it cannot be independent simply because NITDA is connected to the government. However, most data protection authorities are set up by the government, and it is not this ministerial act which determines independence but the operational mechanisms of the body. In this regard, Applicant ought to have demonstrated how the current organizational structure and execution of NITDA undermines its independence as envisaged under the Act.

50. Generally, setting up data protection authorities is the function of government, except that post-set-up, independence must be asserted. In Ghana, for instance, under the Data Protection Act of 2012 (Act 843), the Executive Director of the Data Protection Commission is appointed by the President of the Republic, and its governing board has institutional representatives from the communications and information technology agencies under government. Thus, proof of compromise of independence must be factually asserted and not assumed.

51. The Applicant's qualms with NITDA also appear to stem from its belief that the Supplementary Act's requirement of establishing a Data Protection Authority cannot be achieved by designating existing

institutions to perform its functions. Such that, it is only by establishing a new body that the requirement of independence is met. The Court notes that while setting up a new body may be desirable, it is not a sine qua non to achieving the object of Articles 2 and 14 of the Supplementary Act.

52. As noted earlier, the test of the independence of a body charged with ensuring compliance with a data protection law is not cosmetic or superficial but qualitative. It, therefore, requires a deliberate incision of the organization and operational structures to reach a decisive conclusion. The Applicant needs to provide the evidence necessary to make such a conclusion.

53. The Court further observes that, since the commencement of the action in July 2021, two significant efforts have been undertaken. First is establishing the Nigerian Data Protection Bureau (NDPB) in February 2022 to take over the function of NITDA to administer the NDPR and its implementation framework. The second is introducing a Nigerian Data Protection Bill 2022 in October 2022. Both actions are commended as consistent with the normative approach by other countries towards domesticating the Supplementary Act.

54. There is a practical value to a State having a single comprehensive law to regulate personal data processing and related matters; hence States must strive towards achieving such uniformity. However, the test for whether any framework satisfies the terms of the Supplementary Act would be based on something other than it being contained in a single legislation or necessarily enacted by an act of Parliament. The substance of the framework, regarding protection scope, implementation framework, and redress mechanisms, weigh more than the optics of the framework.

55. On account of the preceding analysis, the Court finds that the Respondent cannot be said to be in breach of its obligation to establish a framework for the protection of personal data under Article 2 or a Data Protection Authority (DPA) under Article 14. Admittedly, the Supplementary Act has not been domesticated through substantive legislation or by creating a new DPA as ordinarily desired; but the current legal regime for the protection of personal data in the Respondent country satisfies the object of the Supplementary Act unless the contrary is proven. Consequently, having failed to prove the contrary, the Applicant's case under this heading fails and is hereby dismissed.

c. ***The issue of compellability of the Respondent to pass a comprehensive framework on data protection.***

56. Respondent submitted that the crux of this matter relates to an alleged failure of the Respondent to honour its obligation by enacting legislation on data privacy under the Supplementary Act. This fact renders the Application incompetent since only Member States can compel the Respondent to pass such legislation.
57. What the Respondent seems to submit is that, were the Respondent to be in breach of its obligation to establish a framework and a DPA, the Applicant's relief for an order compelling it could still not have been granted.
58. The Court has determined that the Respondent has not breached its obligation to establish a legislative framework on data privacy as required by the Supplementary Act. For this reason, the Court does not consider it necessary or desirable to speculate on whether it has the power to order

the Respondent to enact such a legislation had it reached a different conclusion.

X. REPARATIONS

62. The Applicant sought three reliefs captured under paragraph 15 of this judgment which all failed.

63. It is trite law and practice of all human rights enforcement institutions that reparation or compensation is given for violation of human rights that is concrete and real. Where there is no violation, there will be no reparation. In *MRS MODUPE DORCAS AFOLALU v. REPUBLIC OF NIGERIA ECW/CCJ/JUD/15/14 (Unreported),* the court held that *"the principle of reparation constitutes one of the fundamental principles of law regarding liability. It is sufficient that the harm to be repaired must exist in reality, must be directly linked to the victim, and shall be true and capable of being evaluated".*

64. In line with the above principle, it is clear that the Applicant is not entitled to any reparation and the Court so holds.

XI. COSTS

65. Both parties did not pray for costs. Article 66 (1) of the Rules of Court provides, *"A decision as to costs shall be given in the final judgment or in the order, which closes the proceedings."*

66. In addition, Article 66(2) of the Rules of Court provides, *"The unsuccessful party shall be ordered to pay the costs if they have been applied for in the successful party's pleadings."*

67. In light of the provisions of the Rules, the Court holds that parties bear their respective costs since the Respondent, as a successful party, failed to pray for costs.

XII. OPERATIVE CLAUSE

68. For the reasons stated above, the Court sitting in public after hearing both parties:

On jurisdiction

i. **Declares** that it has the competence to adjudicate on the Application;

On admissibility

ii. **Declares** that the Application is admissible;

On Merits

iii. **Declares** that the Respondent did not the Applicant's right to privacy for failure to enact a comprehensive framework on personal data protection;

iv. **Declares that** the Respondent is not in breach of its international obligations under the Supplementary Act of ECOWAS; and

v. **Dismisses** all other declarations or reliefs sought by the Parties

On Costs:

vi. **Orders** the parties to bear their respective costs.

Hon. Justice Edward Amoako **ASANTE** .....

Hon. Justice Gberi-Be **OUATTARA** .....

Hon. Justice Dupe **ATOKI** .....

ASSISTED BY:

Dr. Athanase **ATANNON** .....

Done in Abuja, this 13th Day of March 2023 in English and translated into French and Portuguese.