THE EXTRATERRITORIAL MEDIATOR: WHEN YOUR CLIENT'S DATA CROSSES THE LINE

Adamma Chigozie Isamade*

Abstract

Mediators increasingly operate in complex transnational environments triggering extraterritorial application of multiple, often conflicting, data protection regimes. However, the success of these processes relies on the free and confidential exchange of highly sensitive information, placing Alternative Dispute Resolution (ADR) on a collision course with the expanding reach of global data protection laws. This article examines the legal challenges mediators face when handling cross-border data transfers, the implications of the Singapore Convention on Mediation for data dispute resolution, and the dangerous ***"Clash of Obligations"*** *where a mediator's duty of confidentiality in one state may conflict with an order for disclosure or e-discovery in another. The article argues that mediators must adopt proactive compliance strategies. Ultimately, the article proposes a framework for ethical and legally compliant cross-border mediation practice in the digital age.*

Introduction

Picture this scenario: You are mediating a commercial dispute between a Nigerian technology company and a European distributor. During confidential caucus sessions, both parties share sensitive business data, employee information, and proprietary algorithms stored on cloud servers spanning three continents. Without realizing it, you have become an international data controller subject to multiple extraterritorial data protection regimes. The question is not whether this creates legal obligations, as it does, but rather how mediators can navigate this complex regulatory landscape while preserving the confidentiality that makes mediation effective.

The proliferation of cross-border disputes, coupled with the rapid digitalization of mediation processes accelerated by the COVID-19 pandemic, has created

* ***Adamma Chigozie Isamade***, *Data Protection Professional; Member, Nigerian Bar Association; Institute of Chartered Mediators and Conciliators; Chartered Institute of Arbitrators (UK); Internet Society (Nigeria Chapter). Email: ada.isamade@gmail.com; Tel: +234 802 563 5337.*

unprecedented challenges at the intersection of Alternative Dispute Resolution (ADR) and data protection law[1]. Mediators who once relied primarily on face-to-face meetings and paper documents now routinely handle electronic files, conduct virtual sessions across multiple time zones, and store confidential information on cloud platforms whose physical infrastructure may be scattered across numerous jurisdictions.

This article examines the legal framework governing cross-border data transfers in mediation, focusing on three critical questions: First, when do extraterritorial data protection laws apply to mediators? Second, how can mediators lawfully transfer data across international boundaries while maintaining confidentiality? Third, what practical strategies can mediators adopt to ensure compliance without compromising the efficiency and effectiveness of the mediation process?

The Extraterritorial Reach of Data Protection Laws

Understanding Extraterritoriality in the Digital Context

Extraterritoriality in data protection law refers to the application of a jurisdiction's legal requirements to entities and activities occurring outside its territorial boundaries. This represents a significant departure from traditional international law principles, which generally limit a state's prescriptive jurisdiction to its own territory[2]. The General Data Protection Regulation (GDPR)[3] Article 3(2)[4] serves as a typical example of extraterritorial data protection legislation. This means that a mediator based in Lagos, Singapore, or New York may be subject to GDPR compliance obligations if they process the personal data of individuals physically located in the European Union, even if the mediator has no physical presence or establishment within EU territory. From a mediator's perspective, the practical implications are

[1] Dewi, Sinta and Walters, Robert and Trakman, Leon and Zeller, Bruno, "The Role of International Mediation in Data Protection and Privacy Law - Can It be Effective?" (September 1, 2019). (2019) 30 Australian Dispute Resolution Journal 61, UNSW Law Research Paper No. 19-77

[2] Koloßa, S. (2020). The GDPR's extra-territorial scope: Data protection in the borderless online sphere. *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, 80(4), 791–818. https://www.zaoerv.de/80_2020/80_2020_4_a_791_818.pdf

[3] Regulation (EU) 2016/679, 2016.

[4] Article 3(2) GDPR - applies to the processing of personal data of data subjects who are in the Union by controllers or processors not established in the Union, where processing activities relate to offering goods or services to such data subjects or monitoring their behavior.

clear: geographic location provides no immunity from compliance obligations when handling data of EU residents.

The Nigerian Perspective on Cross-Border Data Transfers

Nigeria's approach to extraterritorial data protection, codified in the Nigeria Data Protection Act (NDPA), 2023[5], takes a different but equally consequential approach. Section 41(1) of the NDPA establishes a default prohibition against transferring personal data outside Nigeria, subject to specific exceptions.

For mediators practicing in or with Nigerian parties, this creates a compliance obligation that operates in the opposite direction from GDPR. A mediator in London handling a dispute involving Nigerian parties must ensure that any transfer of personal data from Nigeria to the UK meets one of the statutory exceptions, such as adequacy of protection, binding corporate rules, standard contractual clauses, or explicit consent after informing data subjects of transfer risks.[6]

Other Jurisdictions and their Requirements

Singapore's Personal Data Protection Act[7], while generally more permissive regarding cross-border transfers, still requires organizations to ensure that recipients provide comparable protection. China's Personal Information Protection Law[8] establishes even more stringent requirements, including security assessments for certain categories of data transfers and localization requirements for critical information infrastructure operators.

The proliferation of these regimes creates what scholars have termed "jurisdictional chaos" in data protection.[9] A single mediation involving parties from multiple jurisdictions may simultaneously trigger compliance obligations under several legal frameworks, each with different requirements for lawful data transfers, distinct

[5] Nigeria Data Protection Act, 2023. https://ndpc.gov.ng/resources/
[6] Aluko & Oyebode. (2023, July 17). Privacy please – Cross border transfer of personal data in Nigeria. https://www.aluko-oyebode.com/insights/cross-border-transfer-of-personal-data-in-nigeria/
[7] Personal Data Protection Act, 2012. https://sso.agc.gov.sg/Act/PDPA2012
[8] Personal Information Protection Law, 2021. https://personalinformationprotectionlaw.com/
[9] Data Privacy Office. (2025, September 23). Navigating the jurisdictional chaos: An international law perspective on the extraterritorial application of data protection laws. https://data-privacy-office.eu/navigating-the-jurisdictional-chaos-an-international-law-perspective-on-the-extraterritorial-application-of-data-protection-laws/

standards for adequacy, and varied enforcement mechanisms. The challenge for mediators is not simply understanding each regime in isolation, but rather developing compliance strategies that satisfy multiple, sometimes conflicting, legal obligations simultaneously.

The Foundational Principle of Mediation Confidentiality

Confidentiality constitutes a cornerstone principle of mediation practice, enabling parties to engage in candid discussions, explore settlement options, and make admissions without fear that their statements will be used against them in subsequent litigation.[10]

The legal foundations for mediation confidentiality vary across jurisdictions but generally derive from statute, procedural rules, professional ethics codes, and contractual agreements between parties. In the European context, Directive 2008/52/EC on certain aspects of mediation in civil and commercial matters establishes confidentiality requirements for cross-border mediations, prohibiting mediators and parties from giving evidence in judicial or arbitration proceedings concerning information arising from or in connection with mediation.[11] Similar protections exist in many common law jurisdictions through "without prejudice" privilege rules and mediation-specific legislation.

Data Protection as a Competing Confidentiality Framework

Data protection law introduces a parallel but distinct confidentiality framework focused specifically on personal information. Under the GDPR, Article 5(1)(f), personal data must be processed "in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures".[12] This obligation, known as the confidentiality and integrity

[10] Via Mediation Centre. (2024, September 9). Confidentiality in mediation. https://viamediationcentre.org/readnews/MTM0OA==/CONFIDENTIALITY-IN-MEDIATION

[11] Directive 2008/52/EC of the European Parliament and of the Council of 21 May 2008 on certain aspects of mediation in civil and commercial matters. (2008). *Official Journal of the European Union*, L 136/3. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0052

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). (2016). *Official Journal of the European Union*, L 119/1. **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679**

principle, creates legal duties that may overlap with, reinforce, or occasionally conflict with mediation confidentiality requirements.

The intersection of these two confidentiality frameworks creates both synergies and tensions. On one hand, mediation's confidentiality commitments align well with data protection's emphasis on limiting access to personal information. Mediators' professional obligations to maintain confidentiality can serve as organisational measures supporting GDPR compliance. On the other hand, data protection law creates new obligations such as responding to data subject access requests, maintaining processing records, and reporting data breaches that may test the boundaries of mediation confidentiality.[13]

Navigating the Practical Tensions

Mediators can adopt several strategies to navigate the tension between mediation confidentiality and data protection transparency. First, explicit contractual provisions in mediation agreements; second, careful data minimisation; third, mediators should distinguish between different categories of information: settlement agreements, process communications, and administrative data as data protection rights may apply differently to these categories; and finally, the forthcoming enforcement of the Singapore Convention on Mediation, which Nigeria ratified in 2023, may influence how courts balance mediation confidentiality against data protection transparency,[14] specifically Article 7 of the Convention.[15]

Legal Mechanisms for Lawful Cross-Border Data Transfers in Mediation

Adequacy Decisions and Whitelisting

The most straightforward mechanism for lawful cross-border data transfers involves adequacy decisions, whereby a data protection authority or commission determines that a foreign jurisdiction provides an adequate level of data protection essentially equivalent to the exporting jurisdiction's standards. Under the NDPA, the Nigeria

[13] Academia.edu. (2019). *The confidentiality intrinsic to mediation and the demand for data protection*. Retrieved from https://www.academia.edu/38738825/THE_CONFIDENTIALITY_INTRINSIC_TO_MEDIATION_AND_THE_DEMAND_FOR_DATA_PROTECTION

[14] IMI Mediation. (2023, December). Nigeria ratifies the Singapore Convention. https://imimediation.org/2023/12/11/nigeria-ratifies-the-singapore-convention/

[15] Article 7 establishes limited grounds for refusing enforcement based on confidentiality considerations, potentially providing guidance on when protecting mediation confidentiality justifies limiting data subject rights.

Data Protection Commission holds exclusive authority[16] to issue adequacy decisions, whether for entire countries, specific sectors, or regions.[17]

Standard Contractual Clauses and Binding Corporate Rules

In the absence of adequacy decisions, Standard Contractual Clauses (SCCs)[18] represent the most widely used mechanism for lawful international data transfers. For mediators, implementing SCCs requires careful attention to roles and relationships. In many mediations, the mediator acts as a data processor, processing personal data on behalf of the parties (controllers) for the limited purpose of facilitating dispute resolution. Cross-border mediations may therefore require controller-to-processor SCCs between each party and the mediator, particularly if the mediator is located in a jurisdiction without an adequacy decision.

Binding Corporate Rules (BCRs) provide an alternative mechanism for multinational organizations, allowing intra-group transfers based on globally applicable data protection policies approved by supervisory authorities. However, BCRs' complexity and resource requirements make them impractical for most mediation practices, which typically operate as independent practitioners or small firms rather than multinational corporate groups.

Derogations for Specific Situations

Data protection regimes recognize that strict transfer restrictions may be impractical in certain circumstances, establishing derogations that permit cross-border transfers based on specific justifications. The NDPA includes derogations, permitting cross-border transfers when explicitly consented to after risk disclosure, necessary for contract performance, required for legal claims, needed to protect vital interests, or justified by important public interest.[19] An additional derogation permits transfers "for the sole benefit of a data subject" where obtaining consent is impractical and the data subject would likely consent if able, potentially relevant for urgent mediations involving incapacitated parties.

[16] Olaniwun Ajayi LP. (2025, May 26). Navigating cross border data transfers – Key insights under Nigeria's data protection laws. https://www.olaniwunajayi.net/blog/navigating-cross-border-data-transfers-key-insights-under-nigerias-data-protection-laws/

[17] Nigeria Data Protection Act, 2023, Section 41.

[18] SCCs are pre-approved contract templates containing data protection obligations that bind data importers in third countries to maintain adequate protection standards.

[19] Nigeria Data Protection Act, 2023, Section 43.

For mediators, the most relevant derogations involve explicit consent and necessity for the establishment, exercise, or defense of legal claims. Explicit consent requires active, informed, and freely given agreement from data subjects specifically for the cross-border transfer, after being informed of potential risks arising from the absence of adequacy or appropriate safeguards. **The Singapore Convention[20] and Data Dispute Mediation**

The Singapore Convention's potential relevance to data protection disputes merits particular attention. As cross-border data flows proliferate, so too do disputes involving data protection compliance, breach notification obligations, processor-controller relationships, and data subject rights. However, several characteristics of data protection disputes create unique challenges under the Singapore Convention framework. First, many data protection laws include mandatory provisions establishing non-waivable rights and obligations. Data subjects' rights to erasure, rectification, and compensation for violations cannot simply be contracted away through mediated settlements. This raises questions about whether settlements that purport to limit or eliminate data subject rights would violate public policy grounds for refusing enforcement under[21] the Convention.

Second, data protection authorities maintain independent enforcement powers and are not bound by private settlements. Therefore, even a successful mediation of a data protection dispute does not prevent regulators from investigating violations and imposing administrative fines. While mediation resolves commercial and relational issues, it cannot fully resolve compliance liability.

Third, the Convention's confidentiality rules[22] clash with data protection's transparency requirements. Data protection laws may mandate disclosure of settlement terms, particularly when the agreement affects data subjects' rights or is requested during an investigation. Therefore, mediators must recognize that complete confidentiality of settlement terms is often unachievable when regulatory interests are involved.

Nigeria's Ratification and Implementation

[20] Singapore Convention on Mediation. (2018). United Nations Convention on International Settlement Agreements Resulting from Mediation. https://www.singaporeconvention.org
[21] Singapore Convention, Article 5(1)(b)(ii)
[22] Singapore Convention, Article 8

Nigeria's ratification of the Singapore Convention in December 2023 positions the country as a regional leader in modern dispute resolution frameworks.[23] However, domestic implementation remains incomplete, and until such implementation occurs, mediators and parties should not assume Nigerian courts can enforce international mediated settlements under the Convention framework.

For cross-border mediations involving Nigerian parties and data, a strategic choice arises: rely on the Singapore Convention for enforcement, or use mechanisms like recording settlements as court consent judgments? The optimal choice depends on the specific jurisdictions, the settlement commitments, and regulatory oversight interests that could complicate purely contractual enforcement.

Practical Compliance Strategies for Mediators

Conducting Data Transfer Impact Assessments

A mediation-specific transfer impact assessment should evaluate: (1) the nature and sensitivity of data to be transferred; (2) the legal framework in the destination jurisdiction; (3) the practical enforceability of any contractual safeguards given the recipient jurisdiction's legal system; and (4) available supplementary measures to mitigate identified risks.

For many mediations, supplementary measures will prove essential. End-to-end encryption of all data in transit and at rest. Pseudonymisation techniques can protect identity while preserving mediation functionality. Data minimisation reduces risk exposure, and access controls limiting who within a mediation can access transferred data, provide additional protection.

Implementing Privacy by Design in Mediation Practice

Practical privacy-by-design measures for mediators include: (1) Using mediation platforms with built-in security (encryption, access controls) instead of generic file shares; (2) implementing data retention schedules to automatically delete information post-mediation; (3) employing need-to-know access so only relevant personnel see confidential materials; (4) conducting privacy impact assessments for high-risk cases (e.g., sensitive data, vulnerable subjects); and (5) maintaining thorough documentation of all processing and compliance measures.

[23] IMI Mediation. (2023, December). Nigeria ratifies the Singapore Convention. https://imimediation.org/2023/12/11/nigeria-ratifies-the-singapore-convention/

Drafting Data Protection-Compliant Mediation Agreements

The mediation agreement must be the data protection foundation, explicitly establishing the legal basis and parameters for data processing. It should clearly address: (1) identification of parties, mediator, and any administrative support staff as controllers or processors; (2) purposes and legal bases for processing personal data; (3) categories of data that may be processed; (4) security measures to protect data; (5) data retention and deletion procedures; (6) mechanisms for cross-border transfers (adequacy, SCCs, derogations); (7) allocation of data protection responsibilities among parties and mediator; and (8) procedures for exercising data subject rights.

For cross-border transfers, the agreement must incorporate or reference SCCs, ensuring all relevant parties execute them. If relying on derogations (like consent or legal claims), the specific, justifying circumstances must be fully documented. In multi-jurisdictional disputes, the agreement must clarify the governing data protection law and detail the conflict resolution mechanism.

Mediators often overlook the risk posed by third-party service providers (e.g., platforms, transcription). Since each vendor is a potential data processor, the mediation agreement must either identify them upfront or establish a procedure for securing parties' consent before engagement. This ensures data protection compliance extends across the entire processing chain, especially for cross-border transfers.

Ethical Considerations and Professional Responsibilities

Duty of Competence in the Digital Age

The Model Standards of Conduct for Mediators, jointly adopted by the American Arbitration Association, American Bar Association, and Association for Conflict Resolution, emphasise that "[a] mediator shall mediate only when the mediator has the necessary competence to satisfy the reasonable expectations of the parties".[24] For cross-border mediations involving international data transfers, reasonable expectations include that the mediator will comply with applicable data protection

[24] Model Standards of Conduct for Mediators. (2005). American Arbitration Association, American Bar Association, and Association for Conflict Resolution. https://icdr.org/sites/default/files/document_repository/Model_Standards_of_Conduct_for_Mediators.pdf

laws, implement appropriate security measures, and not expose parties to regulatory liability through non-compliant data handling.

Mediators must therefore engage in ongoing professional development addressing data protection and cybersecurity issues. This includes understanding the basic frameworks of major data protection regimes, recognising when mediations trigger cross-border transfer obligations, implementing technological solutions for secure data handling, and knowing when to consult with data protection counsel. Institutions offering mediator training should incorporate data protection modules covering these essential competencies.

Informed Consent and Transparency

Informed consent is foundational to both mediation ethics and data protection law. In mediation, it requires parties to understand the process, the mediator's role, and confidentiality limits. For data protection, consent, as a common legal basis for processing, must be freely given, specific, informed, and unambiguous.

In cross-border mediation, transparency is crucial due to unfamiliar data protection risks. Mediators must clearly inform parties about all data processing activities, specifying what data is collected, how it's used and secured, who accesses it, where it's stored and transferred, and how long it's retained.

Conflicts of Interest in Data Handling

Traditional mediation conflict analysis focuses on impartiality and independence. Data protection adds new dimensions: mediators must disclose material relationships concerning data processing, such as platform ownership, data-sharing arrangements, or cloud provider affiliations. This aligns with general disclosure practices while addressing data-specific conflicts increasingly relevant to modern practice.

Conclusion

The intersection of mediation practice and data protection law presents complex challenges that will only intensify as digital transformation continues and cross-border dispute resolution grows. Mediators can no longer treat data protection as a peripheral concern or specialised niche; it has become central to competent, ethical practice in the 21st century.