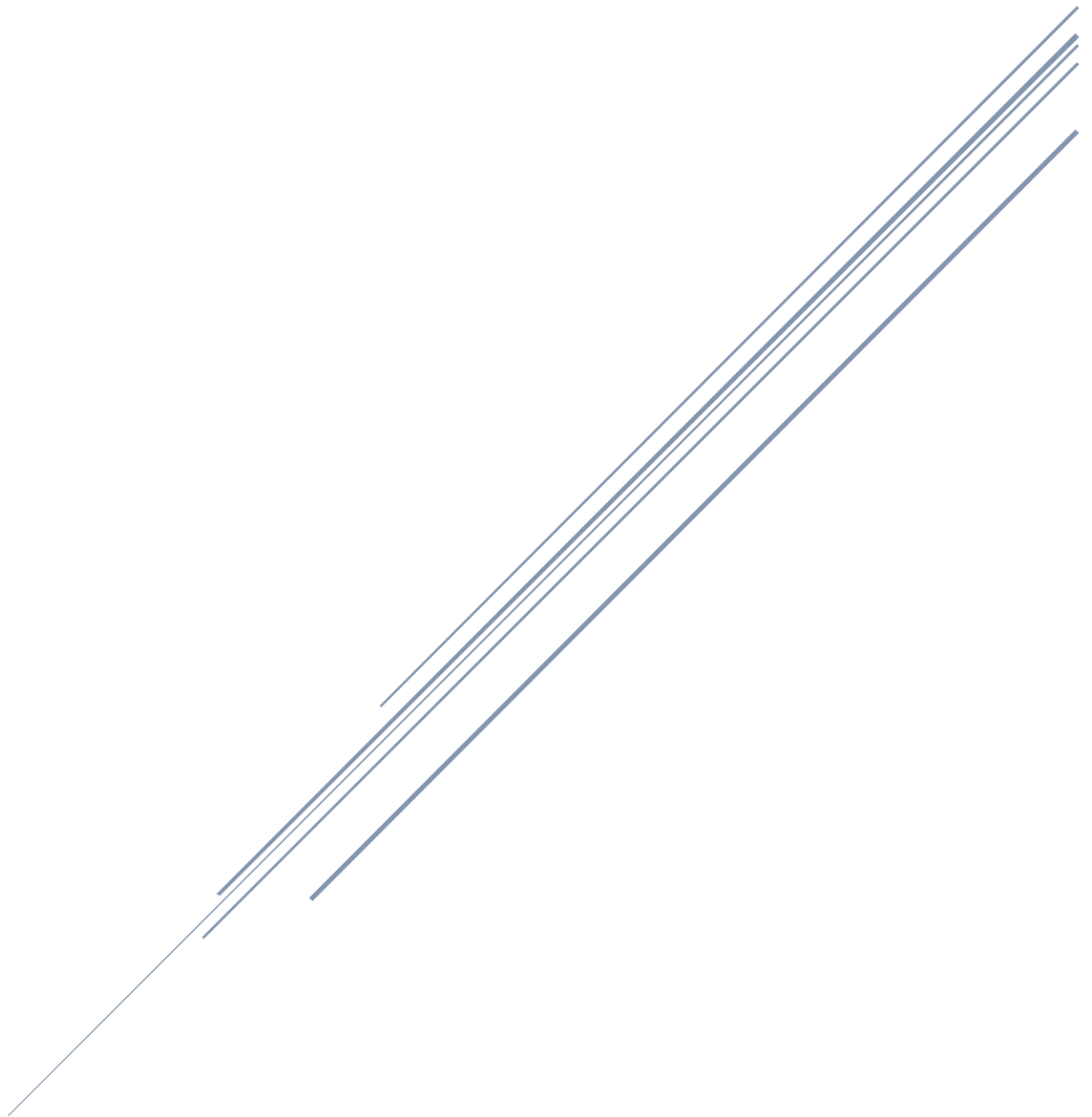


PRIVACY GUIDANCE FOR LAWYERS IN NIGERIA – NBA-SLP



Nigerian Bar Association Section on Legal Practice
Technology and Law Committee

PRIVACY GUIDANCE FOR LAWYERS IN NIGERIA



NIGERIAN BAR ASSOCIATION - SECTION ON LEGAL PRACTICE

FOREWARD

The protection of personal data has become a paramount concern in today's digital age. As custodians of sensitive information, lawyers have a unique responsibility to safeguard the privacy of their clients. This Privacy Guidance for Lawyers in Nigeria is a timely and essential resource for the legal profession.

The document provides clear and practical guidance on the application of the Nigeria Data Protection Act (NDPA) to the practice of law. It highlights the importance of data protection in building and maintaining trust with clients.

I commend the Section on Legal Practice for undertaking this important initiative. By adhering to the principles outlined in this guidance, lawyers can demonstrate their commitment to protecting client confidentiality and complying with legal obligations.

Yakubu Chonoko Maikyau, SAN
President, Nigerian Bar Association

ACKNOWLEDGMENTS

The development of this Privacy Guidance for Lawyers in Nigeria would not have been possible without the invaluable contributions of numerous individuals and organizations. We extend our sincere gratitude to the members of the Nigerian Bar Association Section on Legal Practice whose expertise and dedication were instrumental in shaping the content of this document.

We are particularly indebted to Olumide Babalola, Olaniwun Ajayi LP, Kenna Partners, Tsedaqah Attorneys, Nigerian Institute of Advanced Legal Studies, Gold and Sterling Attorneys, the Dean of the Law Faculty of the university of Ilorin, Damilola Alabi, Uloma Emeyonu, Mabel Nwanosike, Mr. Ehizele, Oyinyechi Ibemere, Oladapo Abudu, Banwo & Ighodalo, Rita Chris Garuba, and Ishola Olatunbosun for their insightful contributions and efforts. Their knowledge and experience were essential in ensuring the comprehensiveness and practical relevance of these Guidelines.

We also acknowledge the support and encouragement of the Nigerian Bar Association leadership, whose vision and guidance have been invaluable in this endeavor.

Finally, we express our appreciation to all those who participated in the consultation process, including members of the legal profession, academia, and industry. Your feedback and suggestions have significantly enhanced the quality of these Guidelines.

EXECUTIVE SUMMARY

This document provides guidance on data protection considerations for legal practitioners in Nigeria, with a focus on compliance with the Nigeria Data Protection Act (NDPA) 2023 and the Rules of Professional Conduct 2023 as they relate to client, employee and other party's information. It highlights the importance of data protection in maintaining client trust, adhering to legal requirements, and mitigating data breach risks.

The document outlines the key principles of the NDPA, including lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. It explains when legal practitioners act as data controllers and data processors, and the lawful bases for processing client data.

The guidance covers data security obligations for legal practitioners, such as implementing strong access controls, encryption, and secure disposal practices. It also addresses data breach notification requirements and the need to establish procedures for identifying, investigating, and reporting breaches.

The document addresses specific privacy considerations for legal practice, including client data collection and storage, cross-border data transfers, the use of third-party service providers, and privacy implications in electronic discovery. It also emphasises the importance of adhering to the Rules of Professional Conduct and clear communication with clients regarding Data Protection.

The document outlines best practices for Data Protection compliance, such as data minimisation, appropriate retention periods, regular risk assessments, staff training, and the conduct of Data Protection Impact Assessments (DPIAs) for high-risk processing activities. It also provides guidance on handling data subject access requests in line with the NDPA.

By understanding and implementing the principles and practices outlined in this document, legal practitioners in Nigeria can ensure the responsible and ethical handling of client data, maintain client trust, and comply with the NDPA's data protection requirements.

TABLE OF CONTENTS

1. Introduction
 - 1.1 Importance of Data Protection in Legal Practice
 - 1.2 Purpose of this Guidance
2. The Nigeria Data Protection Act (NDPA) 2023
 - 2.1 Overview of the NDPA
 - 2.2 Key Definitions
 - 2.3 Key Principles of Data Processing under the NDPA
3. Legal Practitioners and the NDPA
 - 3.1 When do Legal Practitioners Act as Data Controllers?
 - 3.2 When do Legal Practitioners Act as Data Processors?
 - 3.3 Legal Basis for Processing Client Data under the NDPA
 - 3.4 Data Security Obligations for Legal Practitioners
 - 3.5 Data Breach Notification Requirements
4. Specific Privacy Considerations for Legal Practice
 - 4.1 Client Data Collection and Storage Practices
 - 4.2 Cross-Border Data Transfers of Client Data
 - 4.3 Use of Third-Party Service Providers and Technology
 - 4.4 Privacy Considerations in Electronic Discovery and E-disclosure
 - 4.5 Ethical Obligations and Client Communication regarding Data Protection
5. Best Practices for Data Protection Compliance
 - 5.1 Data Minimization and Retention Periods
 - 5.2 Implementing Data Security Measures
 - 5.3 Conducting Data Protection Impact Assessments (DPIAs)
 - 5.4 Data Subject Access Requests and Handling Procedures
6. Appendix
 - Sample Data Breach Notification Template

PRIVACY GUIDANCE FOR LAWYERS IN NIGERIA

1. Introduction

1.1 Importance of Data Protection in Legal Practice

In today's digital age, legal practitioners handle vast amounts of sensitive client data. This data includes personal information such as names, addresses, contact details, financial records, marital information, family information, health status, criminal records, employees' data, other colleagues data, adverse parties' data and confidential communications related to legal matters. Ensuring the privacy and security of this data is important for several reasons:

- **Maintaining Client Trust:** Clients entrust legal practitioners with their most sensitive information. Upholding data privacy demonstrates respect for client confidentiality and builds trust in the attorney-client relationship.
- **Compliance with the Nigeria Data Protection Act (NDPA) 2023:** The NDPA regulates all dealings with personal data including the collection, processing, storage, transfer, and use of personal data. Legal practitioners who handle client data must comply with the Act's provisions to avoid potential penalties and reputational damage.
- **Mitigating Data Breach Risks:** Cybersecurity threats are constantly evolving, accidental or intentional compromise of data and cybersecurity threats are more rampant, and data breaches can have serious consequences for both clients and legal practices. Implementing robust data security measures helps protect client data and minimizes the risk of breaches.

1.2 Purpose of this Guidance

This guidance aims to equip legal practitioners in Nigeria with a clear understanding of their obligations under the NDPA 2023. It outlines key

principles, best practices, and considerations to ensure the responsible and ethical handling of client data throughout the course of legal representation.

2. The Nigeria Data Protection Act (NDPA) 2023

2.1 Overview of the NDPA

The NDPA was signed into law on the 12th day of June 2023. Its main objectives are to regulate processing of personal data, promote privacy of data subjects and ensure that data controllers and data processors fulfil their obligations to data subjects. It regulates the collection, processing, storage, transfer, and use of personal data by organizations operating in Nigeria. It empowers individuals (data subjects) with control over their personal data and mandates organizations (data controllers and processors) to adhere to specific data protection principles.

2.2 Key Definitions

- **Data Breach:** A data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed. This can include both deliberate attacks on data security and accidental incidents, such as lost devices or misdirected emails containing personal data.
- **Data Controller:** The organization that determines the purposes and means of processing personal data. In the context of legal practice, the legal practitioner, law firm or legal department typically acts as the data controller for client data they collect and process.
- **Data Processor:** An organization that processes personal data on behalf of a data controller. For example, a legal practitioner might use a cloud storage service provider to store client data. In this scenario, the cloud service provider acts as a data processor.
- **Data Subject:** The individual to whom the personal data relates. This is the client whose personal data is being collected and processed by the

legal practitioner.

- **Personal Data:** Any information relating to an identified or identifiable natural person. This includes information such as names, addresses, phone numbers, email addresses, images or voice recording, text messages, client's instructions or briefs, spousal or children's data, employees data, financial data, opinions, and biometric data.
- **Processing:** Processing refers to any operation or set of operations performed on personal data, whether by automated means or not. This includes collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing, or destroying personal data.
- **Sensitive Personal Data:** Sensitive personal data, also known as special categories of personal data, refers to information that is particularly sensitive in nature and requires heightened protection. This includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person's sex life or sexual orientation

2.3 Key Principles of Data Processing under the NDPA

The NDPA outlines seven key principles that data controllers must adhere to when processing personal data. Understanding these principles is crucial for legal practitioners to ensure their data handling practices are compliant with the law:

- **Lawfulness, Fairness, and Transparency:** Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject. Clients should be informed about the purposes for which their data is being collected, how it will be used, and their rights under

the NDPA.

Client data should only be processed where there exists a lawful basis to do so, for example, in execution of the client's request for legal services, or where the client has given informed consent or under any other lawful basis recognised by the NDPA.

For transparency, lawyers should publish compliant privacy notices on their website and mount conspicuous CCTV notices where such is used in their offices

- **Purpose Limitation:** Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes. Legal practitioners should only collect the minimum amount of personal data necessary for the specific legal matter they are handling and should only use clients' data for the disclosed purpose of collection. For example, when sharing draft processes, client's personal data must be deleted from such processes before sharing as precedents.
- **Data Minimization:** Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. Legal practitioners should avoid collecting unnecessary personal data and regularly review their data holdings to delete outdated or irrelevant information.
- **Accuracy:** Personal data must be accurate and, where necessary, kept up to date. Legal practitioners should have procedures in place to ensure client, employee and 3rd party data is accurate and updated as necessary.
- **Storage Limitation:** Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Legal practitioners should establish data retention policies that outline appropriate retention periods for different types of client data. More detail on data retention is provided in Section 5.1.
- **Integrity and Confidentiality:** Personal data must be processed in a

manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organizational measures. Legal practitioners must implement robust data security measures to safeguard client data (addressed further in Section 3.4). This includes policies and organisation measures like filing and archiving procedure, safe keeping, access control etc.

- **Accountability:** The data controller is accountable for, and must be able to demonstrate, compliance with these principles. Legal practitioners should have documented data protection policies and procedures in place and be able to demonstrate their adherence to the NDPA.

3. Legal Practitioners and the NDPA

3.1 When do Legal Practitioners Act as Data Controllers?

Generally, since lawyers are instructed by clients, and are duty-bound to act under such instructions. However, lawyers are professionals who are trained to make certain decisions on the kinds of (personal) information necessary and how they used to carry out the client's instructions, this qualifies them as 'data controllers. A typical example is when they use third-party service providers to store or manage client data. Here are some examples:

- **Cloud Storage Services:** Utilizing cloud-based platforms to store client documents and electronic files.
- **Email and Collaboration Tools:** Employing email providers or collaboration platforms that involve storing client data on their servers.
- **Document Review Tools:** Utilizing software for electronic discovery or document review that may require uploading client data.

When acting as a data controller, the legal practitioner has a responsibility to ensure the third-party service provider maintains adequate data protection safeguards (addressed further in Section 4.3).

3.2 When do Legal Practitioners Act as Data Processors?

In very limited circumstances lawyers can act as data processors, such as if a client retained a legal practitioner for the express purpose of processing data. Examples include:

- where a client instructs a law firm to act as trustees/executors of a Will with clear instructions on what to do with personal data of beneficiaries
- where a law firm is appointed as collection agents with clear instructions on data processing;
- Where a law firm acts as a facility manager;
- Where a corporate client provides a law firm with a list of their vendors with clear instructions on the purpose and use of the information therein.

3.3 Legal Basis for Processing Client Data under the NDPA

The NDPA outlines lawful grounds for processing personal data. This means that personal data must not be processed except under one of the lawful grounds, otherwise the processing becomes unlawful. Legal practitioners must identify the most appropriate lawful basis for processing client data in each situation. Here are some common lawful bases applicable to the legal profession:

- **Contractual Necessity:** Processing client data is necessary for the performance of a contract with the client (e.g., providing legal representation in a court case).
- **Legal Obligation:** Processing is necessary for compliance with a legal obligation to which the data controller is subject (e.g., anti-money laundering regulations requiring client identity verification).
- **Legitimate Interests:** Processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, except

where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This might include using client data for conflict checks, internal quality control measures, or debt collection purposes, provided it's balanced with client privacy rights.

- **Vital interest:** In the event a clients or his/her relatives are incapable (as a result of illness or accident) of giving consent to certain processing activities which are not covered by the client's instructions, the vital interest kicks in.

It's crucial for legal practitioners to understand and document the lawful basis for processing different types of client data.

3.4 Data Security Obligations for Legal Practitioners

The NDPA mandates data controllers to implement appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing and accidental loss, destruction, or damage. Here are some key considerations for legal practitioners to ensure data security:

- **Strong Password Policies and Access Controls:** Implement strong password policies and restrict access to client data, including case files, only to authorized personnel on a need-to-know basis.
- **Use of Official Email:** Ensure that work-related emails and other communication, particularly those that concern or relate to personal data of clients, employees or any third party are done using official email and communication accounts. This ensures that the information is retained in accounts which the lawyer/law firm/legal department controls and are not accessed by persons who are no longer under the control of the law firm/legal department.
- **Data Encryption:** Encrypt sensitive client data both at rest and in transit.
- **Regular Security Audits and Staff Training:** Conduct regular security audits to identify vulnerabilities and provide staff training on data security best practices and procedures for handling client data.

- **Secure Disposal of Electronic and Physical Data:** Implement secure methods for disposing of electronic devices and physical documents containing client data to prevent unauthorized access.
- **BYOD and Remote Work Policies:** Law firms and legal departments should ensure that they have appropriate Bring-Your-Own-Device (BYOD) and remote-work policies and procedures. A BYOD policy should outline security measures, data ownership, device management, and employee responsibilities to protect sensitive information. The same should apply to remote work policies.

3.5 Data Breach Notification Requirements

The NDPA mandates data controllers to notify the Nigeria Data Protection Commission (NDPC) and data subjects of data breaches that pose a high risk to the rights and freedoms of data subjects. Legal practitioners must establish procedures to:

- **Identify and Investigate Data Breaches:** Have a system in place to detect and investigate potential data breaches promptly.
- **Assess Risk:** Evaluate the severity of the data breach and its potential impact on data subjects' rights and freedoms.
- **Report to NDPC:** Report high-risk data breaches to NDPC within the timeframe stipulated by the NDPA.
- **Notify Data Subjects:** Inform affected data subjects about the data breach in a timely manner and provide clear recommendations to mitigate potential risks.

3.6. Data Breaches that a Law Firm/Legal Department may Encounter

Below are examples of data breaches that a law firm, lawyer or legal department may encounter. The list is not exhaustive.

- **Phishing attacks:** An employee falls for a sophisticated phishing email and inadvertently provides login credentials, giving unauthorized access

to client files.

- **Lost or stolen devices:** A lawyer's laptop containing unencrypted client data is stolen from their car or left behind in a public place.
- **Insider threats:** A disgruntled employee deliberately accesses and leaks sensitive client information.
- **Ransomware attacks:** The firm's computer systems are infected with ransomware, encrypting all client files and demanding payment for their release.
- **Misconfigured cloud storage:** A cloud storage bucket containing client documents is accidentally set to public, allowing anyone on the internet to access the files.
- **Unsecured file transfer:** Sensitive client documents are sent via unsecured email instead of through encrypted channels.
- **Physical document theft:** Paper files containing client information are stolen from the office or during transit.
- **Unauthorized access:** A hacker exploits a vulnerability in the firm's network security, gaining access to the case management system.
- **Improper disposal:** Old computers or hard drives containing client data are disposed of without proper data wiping procedures.
- **Third-party vendor breach:** A breach occurs at a third-party service provider (e.g., e-discovery platform, cloud storage provider) used by the firm, compromising client data.
- **Misdirected communications:** Confidential client information is accidentally sent to the wrong recipient via email or fax.
- **Social engineering:** An attacker impersonates a client or colleague over the phone, tricking a staff member into revealing sensitive information.

4. Specific Privacy Considerations for Legal Practice

4.1 Client Data Collection and Storage Practices

- **Collect Only Minimum Necessary Data:** Only collect the minimum amount of personal data necessary for the specific legal matter you are handling. Avoid collecting unnecessary or irrelevant information about your clients.
- **Obtain Informed Consent:** Obtain clear and informed consent from clients for the collection and processing of their personal data. This consent should explain the purposes for data processing, how the data will be used, and the data subject's rights under the NDPA.
- **Transparent Data Retention Policies:** Establish clear and transparent data retention policies that outline how long different types of client data will be stored. These policies should be communicated to clients and regularly reviewed to ensure outdated data is deleted. (More details in Section 5.1)
- **Secure Storage and Transmission Practices:** Store and transmit client data securely using appropriate safeguards. This may involve cloud storage with strong encryption, secure physical document storage facilities, and access controls to prevent unauthorized use.

4.2 Cross-Border Data Transfers of Client Data

Where a Legal practitioner engages in communications or provides services that involve unusual flow of personal data to entities outside Nigeria, this is known as cross-border data transfer or transborder flow of data. In this case, the lawyer is required to, in addition to measures already previously indicated as required for the handling of personal data, do the following:

- **Be Aware of Restrictions:** The NDPA prohibits transferring client data to countries with inadequate data protection safeguards. Research the data protection laws of the destination country before transferring any

client data.

- **Transfer Mechanisms:** If transferring data outside Nigeria, implement appropriate transfer mechanisms approved by NDPC, such as standard contractual clauses, encryption, recording the basis for transfer, etc.
- **Client Consent:** In some cases, you may need to obtain specific informed consent from clients before transferring their data outside Nigeria.

4.3 Use of Third-Party Service Providers and Technology

- **Due Diligence:** Conduct thorough due diligence on third-party service providers before using their services to store or process client data. Evaluate their data security practices and ensure they comply with the NDPA.
- **Data Processing Agreements:** Enter into written agreements with third-party service providers that clearly define data protection responsibilities. These agreements should address data security measures, data retention periods, ownership and control, and the service provider's obligations in case of a data breach.
- **Secure Data Transfer Protocols:** Ensure secure data transfer protocols are in place when using cloud-based technologies or transferring data to third-party service providers.

4.4 Privacy Considerations in Electronic Discovery and E-disclosure

- **Data Minimization:** During electronic discovery, employ data minimization techniques to identify and segregate only the relevant personal data necessary for the legal matter. Avoid collecting and processing excessive amounts of irrelevant data.
- **Balancing Disclosure:** Balance disclosure requirements with the privacy rights of data subjects. Only disclose personal data that is demonstrably relevant and necessary for the legal proceedings.
- **Data Anonymisation/Pseudonymisation:** Consider anonymizing

personal data whenever possible during e-disclosure, particularly for sensitive information not directly relevant to the case.

4.5 Ethical Obligations and Client Communication regarding Data Protection

- **Rules of Professional Conduct (RPC):** Lawyers are required to adhere to the provisions of the Rules of Professional Conduct for Legal Practitioners 2023 (RPC). While the RPC does not have specific chapters dedicated solely to data protection and security, the rules establish principles that indirectly address these concerns. These include

Rule 1 - Maintaining the Integrity of the Profession: Lawyers are obligated to uphold the integrity of the legal profession, which includes maintaining ethical standards regarding client data.

Rule 14 - Duty to the Client: This rule emphasizes a lawyer's duty to act in the best interests of their client, which includes protecting their confidentiality.

Rule 19 - Confidentiality: This core rule ensures client confidentiality. Lawyers cannot disclose client information without informed consent, with some exceptions permitted by law.

Rule 29 - Record Keeping: This rule mandates lawyers to maintain accurate and complete records for their clients. However, it doesn't explicitly address data security measures.

- **Nigerian Bar Association (NBA) Guidelines:** Adhere to any Data Protection guidelines issued by the Nigerian Bar Association (NBA) regarding the handling of client data.
- **Clear Communication:** Communicate Data Protection policies and practices to clients in a clear, concise, and easily understandable manner.

This can be achieved through client engagement letters, website privacy notices, or other communication channels.

- **Client Inquiries:** Address client inquiries and concerns regarding their Data Protection rights promptly and in a professional manner. Provide clients with clear information on how to exercise their data subject rights under the NDPA (covered in Section 6).

5. Best Practices for Data Protection Compliance

5.1 Data Minimization and Retention Periods

As mentioned earlier, the NDPA emphasizes the principle of data minimization. Legal practitioners should only collect the minimum amount of personal data necessary for the specific legal representation and retain it for no longer than is necessary. Here are some factors to consider when determining appropriate data retention periods:

- **Legal and Regulatory Requirements:** Certain laws or regulations may mandate specific retention periods for certain types of client data (e.g., anti-money laundering regulations). Identify and comply with any such legal obligations. Rule 10(5) of the Legal Practitioners' Account Rules 1964, for example, requires legal practitioners to 'preserve for at least six years from the date of the last entry therein all books, accounts and records kept by him.'
- **Statute of Limitations:** The statute of limitations defines the timeframe within which legal proceedings can be initiated for different types of claims. It's generally advisable to retain client data relevant to potential legal claims for the duration of the applicable statute of limitations period plus a reasonable buffer.
- **Business Needs and Ethical Considerations:** Consider legitimate business needs for retaining client data, such as conflict checking, internal quality control, or historical reference for future client matters.

Balance these needs with the privacy rights of data subjects and avoid retaining data indefinitely.

Here is a suggested approach to data retention periods (not exhaustive):

- **Active Client Files:** Retain for the duration of the legal representation and the applicable statute of limitations period.
- **Inactive Client Files:** After the statute of limitations has expired, consider factors like potential future representation or historical reference needs. You may anonymize (for example, by redaction) or securely dispose of data after a reasonable period (e.g., 5-7 years).
- **Financial Records and Transaction Data:** Adhere to legal and regulatory requirements, which may mandate longer retention periods (e.g., 5-10 years).
- **Marketing and Contact Information:** Retain only for as long as necessary for marketing purposes and in accordance with consent obtained. Consider offering opt-out mechanisms for clients who no longer wish to receive communications.

Remember: These are suggestions, and the appropriate retention period will vary depending on the specific circumstances. Regularly review your data and delete outdated information that is no longer required.

5.2 Implementing Data Security Measures

Robust data security measures are crucial for protecting client data and minimizing the risk of data breaches. Here are some best practices for legal practitioners:

- **Conduct Regular Risk Assessments:** Conduct regular risk assessments to identify potential vulnerabilities in your data security practices. This

may involve assessing your IT systems, physical security measures, and staff procedures for handling data.

- **Train Staff on Data Security:** Train staff on data security best practices and procedures for handling client data. This training should cover topics such as password hygiene, data encryption, recognizing phishing attempts, and reporting data security incidents.
- **Update Software and Applications:** Regularly update software and applications used to store or process client data to ensure they have the latest security patches and are protected against known vulnerabilities.
- **Engage Cybersecurity Professionals:** Retain the services of qualified cybersecurity experts to enhance your data security measures. These professionals can conduct regular security audits, implement robust protection systems, provide ongoing monitoring and support, and keep your defences up-to-date against evolving cyber threats. Their expertise is crucial for identifying vulnerabilities, responding to incidents, and ensuring compliance with data protection regulations, thereby demonstrating due diligence in safeguarding client data.

5.3 Conducting Data Protection Impact Assessments (DPIAs)

The NDPA may require legal practitioners to conduct a DPIA for high-risk processing activities that could significantly impact the rights and freedoms of data subjects. A DPIA is a systematic process that helps identify and mitigate potential privacy risks associated with data processing activities. Here are some situations where a DPIA may be advisable:

- Processing sensitive personal data, such as health information or financial data.
- Using new or emerging technologies for data processing, such as artificial intelligence or facial recognition.
- Data processing activities that involve large-scale data collection or profiling of individuals.

5.4 Data Subject Access Requests and Handling Procedures

The NDPA grants data subjects a right to access their personal data held by a data controller and to request rectification of data, deletion of personal data, objection to the processing of personal data, or its transmission from one data controller to another. Legal practitioners should establish clear procedures for handling data subject access requests within the timeframes outlined in the NDPA. This typically involves:


- **Identifying Requests:** Implement procedures to receive and identify data subject access requests promptly.
- **Verification:** Verify the identity of the data subject requesting access before processing the request.
- **Providing Access and Making Relevant Adjustment:** If the request is valid, provide the data subject with a copy of their personal data, where requested, in a clear and understandable format where the request is to make an adjustment or deletion, such adjustment or deletion should be made promptly and the client notified.
- **Responding to Requests:** Even if the request is denied, provide the data subject with a clear explanation for the denial and their right to complain to NDPC.

Signed:



Yakubo Chonoko Maikyau, OON, SAN

President, NBA



Boma Alabi, OON, SAN

Chairman, NBA-SLP

Fernandez Marcus-Obiene

Chairman, NBA-SLP Tech & Law Committee

Appendix

Sample Data Breach Notification Template To:

Nigeria Data Protection Commission (NDPC)

From: [Name of Law Firm]

Date: [Date]

Subject: Data Breach Notification - [Brief Description of Breach]

Introduction

This letter serves as a formal notification of a data breach that occurred on [Date of Breach] involving personal data held by [Name of Law Firm]. We are committed to protecting the privacy of our clients and take data security breaches very seriously.

Nature of the Breach

[Provide a brief description of the nature of the data breach. This may include details such as the type of data affected (e.g., names, email addresses, Social Security numbers), the approximate number of individuals affected, and the suspected cause of the breach (e.g., hacking incident, malware infection).]

Steps Taken in Response

[Outline the steps taken by the law firm in response to the data breach. This may include actions such as containing the breach, investigating the incident, notifying law enforcement (if applicable), and implementing remedial measures to strengthen data security.]

Affected Data Subjects

[Indicate the approximate number of data subjects affected by the breach. If

possible, specify the categories of data subjects impacted (e.g., all clients, specific practice group clients).]

Risk Assessment

[Briefly assess the potential risks to the rights and freedoms of data subjects as a result of the data breach.]

Communication with Data Subjects

[Explain how the law firm will communicate with affected data subjects regarding the data breach. This may involve sending email notifications, posting a notice on the law firm's website, or other communication channels.]

Contact Information

For any questions or concerns regarding this data breach notification, please contact:

[Name of Contact Person] [Email Address] [Phone Number]

We apologize for any inconvenience caused by this data breach and are committed to taking all necessary steps to protect client data in the future.

Sincerely,

[Name of Law Firm Representative] [Signature] [Print Name]

Important Note: This is a sample template, and the specific content of the data breach notification will vary depending on the circumstances of the breach.