ESHER & MAKARIOS DATA PROTECTION POLICY

1.0. INTRODUCTION

In the course of its operations, Esher & Makarios will gather and use certain information about clients, employees and other persons.

This policy describes how such data must be collected, handled and stored to meet the Firm's data protection standards — and to comply with the Nigeria Data Protection Regulation 2019 (NPDR).

1.1. Policy Rationale

This data protection policy ensures Esher & Makarios:

- Complies with data protection law and follows good practice
- Protects the privacy rights of clients and members of staff
- Is open about how it stores and processes individuals' and organisations' data
- Protects itself from the risks of a data breach

2.0. NIGERIA DATA PROTECTION REGULATION

Nigeria Data Protection Regulation 2019 prescribes how firms/organisations — including Esher & Makarios - must collect, handle and store personal information.

These provisions apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The NPDR is underpinned by the following important principles. Data must:

1. be collected and processed in accordance with specific, legitimate and lawful purpose consented to by the Data Subject; provided that, further processing of data may be done only for archiving, scientific research, historical research or statistical purposes for public interest;

2. be collected without prejudice to the privacy and dignity of human person;
3. be adequately secured against breaches such as theft, viral attacks, manipulation or damage of any kind;
4. be stored for only the purpose and period for which it is intended;
5. be processed fairly and lawfully;
6. be obtained only for specific, lawful purposes; and
7. may be for archiving, scientific research historical research or statistical purposes for public interest.

   Esher & Makarios subscribes to and shall use its best endeavours to uphold the foregoing principles.

2.1. People, Risks and Responsibilities

Policy Scope

This policy applies to:

- Esher & Makarios
- All staff and volunteers of/at Esher & Makarios
- All vendors, contractors, suppliers and other people/organisations working on behalf of Esher & Makarios

It applies to all data that the Firm holds relating to identifiable individuals/organisations, even if that information technically falls outside of the Nigeria Data Protection Regulation 2019. This can include:

- Names of individuals
- Postal and residential addresses
- Email addresses
- Telephone numbers
- Medical records
- Financial information
- Any other information relating to individuals/organisations

2.2. Responsibilities

Everyone who works for or with Esher & Makarios has responsibility for ensuring data is collected, stored and handled appropriately and securely.

Each member of staff that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

In addition to the foregoing:

- The **Lead Partner** is ultimately responsible for policy formulation and compliance with legal requirements.

- **The Practice Administrator** shall be particularly responsible as the Firm's Data Protection Officer and particularly for:
    - Keeping the Firm's management updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the individuals/organisations covered by this policy.
    - Handling data protection questions and concerns from members of staff and anyone else covered by this policy.

- Dealing with subject access requests.
- Checking and approving any contracts or agreements with third parties that may handle the Firm's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet high quality security standards.
- Ensuring the performance of regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the Firm's is considering using to store or process data.
- Approving any data protection statements attached to communications such as emails and letters.

2.3 General Staff Guidelines

- All employees must be informed at the start of their employment about the obligation to maintain personal data privacy. This obligation shall remain in force even after their employment has ended.
- The only employees able to access data covered by this policy should be those who need it solely for official purposes.
- Data must not be shared informally. When access to confidential information is required, employees can request it from the Practice Administrator.
- Esher & Makarios will provide regular training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below:
    - Strong passwords must be used and they should never be shared under any circumstance.
    - Personal data should not be disclosed to unauthorised persons, either within the Firm or externally.
    - Data should be regularly reviewed and updated. If it is found to be out of date or no longer required, it should be deleted and disposed of.

- Employees should request help from the Practice Administrator if they are unsure about any aspect of data protection.

3.0. DATA STORAGE

When data is stored on paper, it should be kept in a secure place where unauthorised persons are unable to access it.

These guidelines also apply to data that is usually stored electronically but has been printed out:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised persons could see them.
- Data printouts must be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between members of staff.
- If data is stored on removable media (like a USB/flash drive), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the Firm's standard backup procedures.

- Data should never be saved directly to Computers or laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

3.1. Data Use

Esher & Makarios owes a duty of care to ensure that clients' information are kept securely from the risk of loss, corruption, unauthorised/unlawful disclosure or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked/minimised when left unattended.
- Personal data must never be shared informally.
- Data must be encrypted before being transferred electronically.
- Staff should ensure that written authorisation is sought from the Practice Administrator before sharing clients' information.
- Employees should never save copies of the Firm's data/documents to their own computers.
- Data will be held in as few places as necessary. Employees are not allowed to create additional data sets.

3.2. Data Accuracy

Esher & Makarios will take reasonable steps to ensure that data is accurate and up-to-date. In this regard, Esher & Makarios will:

- ensure that any data collected and/or processed is accurate and not misleading in a way that could be harmful;
- ensure that data is kept updated at all times;
- make judicious efforts to correct/delet eany data that is found to be inaccurate.

3.3. Data Subject Access Requests

Clients and employees whose data are being stored by Esher & Makarios have a right to the following:

- Ask what information the Firms holds about them and why.
- Access to their data being stored by the Firm.
- Be informed how such data is being kept up-to-date.
- Be informed how the Firm is meeting its data protection obligations.

4.0. DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, data may be disclosed under compulsion of law. In such circumstances, Esher & Makarios will disclose requested data. However, the Data Protection Officer will ensure the request is legitimate and must seek authorisation from the Lead Partner in line with the Firm's data release policy.

For more information, contact us on:

info@esherandmakarioslaw.com

234-1-3428150