PILOT SECURITIES LIMITED
(Member of The Nigerian Stock Exchange)

DATA SUBJECT ACCESS REQUEST POLICY

1 About this Policy: scope, purpose and users

1.1 This procedure sets out the key features regarding handling or responding to requests for access to personal data made by data subjects, their representatives or other interested parties. This procedure will enable Pilot Securities Limited (further: "Company") to comply with legal obligations, provide better customer care, improve transparency, enable individuals to verify that information held about them is accurate, and increase the level of trust by being open with individuals about the information that is held about them.

1.2 This procedure applies broadly across all entities or subsidiaries owned or operated by the Company but does not affect any state or local laws or regulations which may otherwise be applicable.

1.3 This procedure applies to employees that handle data subject access requests such as the Data Protection Officer.

2 Data Subject Access Request (DSAR)

2.1 A Data Subject Access Request (DSAR) is any request made by an individual or an individual's legal representative for information held by the Company about that individual. The Data Subject Access Request provides the right for data subjects to see or view their own personal data as well as to request copies of the data.

2.2 A Data Subject Access Request must be made in writing. In general, verbal requests for information held about an individual are not valid DSARs.

2.3 A Data Subject Access Request can be made via any of the following methods: email or post. DSARs made on-line must be treated like any other Data Subject Access Requests when they are received, though the Company will not provide personal information via social media channels.

3 **The Rights of a Data Subject**

The rights to data subject access include the following:

3.1 Know whether a data controller holds any personal data about them.

3.2 Receive a description of the data held about them and, if permissible and practical, a copy of the data.

3.3 Be informed of the purpose(s) for which that data is being processed, and from where it was received.

3.4 Be informed whether the information is being disclosed to anyone apart from the original recipient of the data; and if so, the identity of those recipients.

3.5 The right of data portability. Data subjects can ask that their personal data be transferred to them or a third party in machine readable format (Word, PDF, etc.). However, such requests can only be fulfilled if the data in question is: 1) provided by the data subject to the Company, 2) is processed automatically and 3) is processed based on consent or fulfilment of a contract.

3.6 If the data is being used to make automated decisions about the data subject, to be told what logic the system uses to make those decisions and to be able to request human intervention.

The Company must provide a response to data subjects requesting access to their data within 30 calendar days of receiving the Data Subject Access Request unless local legislation dictates otherwise.

4 **Requirements for a valid DSAR**

4.1 In order to be able to respond to the Data Subject Access Requests in a timely manner, the data subject should:

(a) Submit his/her request using a Data Subject Access Request Form.

(b) Provide the Company with sufficient information to validate his/her identity (to ensure that the person requesting the information is the data subject or his/her authorized person).

4.2 Subject to the exemptions referred to in this document, the Company will provide information to data subjects whose requests are in writing (or by some other method explicitly permitted by the local law), and are received from an individual whose identity can be validated by Company.

4.3 However, Company will not provide data where the resources required to identify and retrieve it would be excessively difficult or time-consuming. Requests are more likely to be successful where they are specific and targeted at particular information.

4.4 Factors that can assist in narrowing the scope of a search include identifying the likely holder of the information (e.g. by making reference to a specific department), the time period in which the information was generated or processed (the narrower the time frame, the more likely a request is to succeed) and being specific about the nature of the data sought (e.g. a copy of a particular form or email records from within a particular department).

5 DSAR process

5.1 Request

Upon receipt of a DSAR, the Data Protection Team will log and acknowledge the request. The requestor may be asked to complete a Data Subject Access Request Form to better enable the Company to locate the relevant information.

5.2 Identify verification

The Data Protection Team needs to check the identity of anyone making a DSAR to ensure information is only given to the person who is entitled to it. If the identity of a DSAR requestor has not already been provided, the person receiving the request will ask the requestor to provide two forms of identification, one of which must be a photo identity and the other confirmation of address.

If the requestor is not the data subject, written confirmation that the requestor is authorized to act on behalf of the data subject is required.

5.3 Information for DSAR

Upon receipt of the required documents, the person receiving the request will provide the Data Protection Team with all relevant information in support of the DSAR. Where the Data Protection Team is reasonably satisfied with the information presented by the person who received the request, the Data Protection Officer will notify the requestor that his/her DSAR will be responded to within 30 calendar days. The 30 day period begins from the date that the required documents are received. The requestor will be informed by the Data Protection Team in writing if there will be any deviation from the 30 day time-frame due to other intervening events.

5.4 **Review of Information**

The Data Protection Team composed of cross department representative will collate the relevant and required information as requested in the DSAR.

The Data Protection Team must ensure that the information is reviewed/received by the imposed deadline to ensure the 30 calendar day time-frame is not breached. The Data Protection Officer will ask the relevant department to complete a "Data Subject Disclosure Form" to document compliance with the 30 day requirement.

5.5 **Response to access requests**

The Data Protection Team will provide the finalized response together with the information retrieved and/or a statement that the Company does not hold the information requested, or that an exemption applies.

The Data Protection Team will ensure that a written response will be sent back to the requestor. This will be via email, unless the requestor has specified another method by which they wish to receive the response (e.g. post).

The Company will only provide information via channels that are secure. When hard copies of information are posted, they will be sealed securely and sent by recorded delivery.

5.6 **Archiving**

After the response has been sent to the requestor, the DSAR will be considered closed and archived by the Data Protection Team.

6 Exemptions

6.1 An individual does not have the right to access information recorded about someone else, unless they are an authorized representative.

6.2 The Company is not required to respond to requests for information unless it is provided with sufficient details to enable the location of the information to be identified, and to satisfy itself as to the identity of the data subject making the request.

6.3 In principle, the Company will not normally disclose the following types of information in response to a Data Subject Access Request:

6.3.1 Information about other people – A Data Subject Access Request may cover information which relates to an individual or individuals other than the data subject. Access to such data will

not be granted, unless the individuals involved consent to the disclosure of their data.

6.3.2 Repeat requests – Where a similar or identical request in relation to the same data subject has previously been complied with within a reasonable time period, and where there is no significant change in personal data held in relation to that data subject, any further request made within a six month period of the original request will be considered a repeat request, and the Company will not normally provide a further copy of the same data

6.3.3 Publicly available information – The Company is not required to provide copies of documents which are already in the public domain.

6.3.4 Opinions given in confidence or protected by copyright law – The Company does not have to disclose personal data held in relation to a data subject that is in the form of an opinion given in confidence or protected by copyright law.

7 DSAR Refusals

There are situations where individuals do not have a right to see information relating to them. For instance:

7.1 If the information is kept only for the purpose of statistics or research, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved.

7.2 Requests made for other, non-data protection purposes can be rejected.

7.3 If the responsible person refuses a Data Subject Access Request on behalf of the Company, the reasons for the rejection must be clearly set out in writing. Any individual dissatisfied with the outcome of his/her Data Subject Access Request is entitled to make a request to the Data Protection Officer to review the outcome.

8 Responsibilities

8.1 The overall responsibility for ensuring compliance with a DSAR rests with the Data Protection Officer.

8.2 If the Company acts as a data controller towards the data subject making the request then the DSAR will be addressed based on the provisions of this procedure.

8.3 If the Company acts as a data processor the Data Protection Officer will forward the request to the appropriate data controller on whose behalf the Company processes personal data of the data subject making the request.