DRAFT OPEN BANKING DIRECTIVE FOR REGULATED FINANCIAL INSTITUTIONS

BANK OF GHANA

DECEMBER 2024

TABLE OF CONTENT

1.0 Preamble

This Open Banking Directive is issued pursuant to the authority of the Bank of Ghana ("the Bank"), under section 4(1)(e) of the Bank of Ghana Act, 2002 (Act 612) as amended and Sections 3(2)(c), 3(2)(i) under the Payment Systems and Services Act, 2019 (Act 987),the provisions of section 3(2)(b), 3(2)(d) of the Banks and Specialized Deposit Taking Institutions Act, 2016, (Act 930), the provisions of the Data Protection Act, 2012, (Act 843), and the provisions of the Cyber Security Act, 2020 (Act 1038), to facilitate the sharing of customer-consented financial data amongst Regulated Financial Institutions (RFIs) .

The Bank recognized the need to develop this Open Banking Directive in furtherance of its policy objective, which is in line with its function of formulating, monitoring, and reviewing policies on the payment ecosystem.

The Bank collaborated with key stakeholders to define an optimal Open Banking Directive that is well suited to Ghana's financial ecosystem, prevailing realities and hereby issues this Open Banking Directive in Ghana.

2.0 Abbreviations

API	Application Programming Interface
AML/CFT	Anti-Money Laundering/Combating the Financing of Terrorism
CDD	Customer Due Diligence
DEMIs	Dedicated Electronic Money Issuers
FICSOC	Financial Industry Command Security Operations Centre
OpenDX	Open Data Exchange
KYC	Know Your Customer
MFA	Multi Factor Authentication
ML/TF/P	Money Laundering/Terrorism Financing & Proliferation of Weapons of mass Destruction
PFTSPs	Payment and Financial Technology Service Providers
PSPs	Payment Service Providers
RFI	Regulated Financial Institution
SOC	Security Operations Centre
TPPs	Third Party Providers

VAPT	Vulnerability Assessment and Penetration Test

3.0 Introduction

This Open Banking Directive is an innovative blueprint aimed at enhancing the current banking and financial landscape. Developed by the Bank of Ghana, this directive serves as a roadmap for RFIs to securely share customer-consented data with each other through Application Programming Interfaces (APIs).

The central point of this Directive lies in the proposition of providing an enabling environment for customers, herein referred to as Data Subjects, of financial institutions, to access a myriad of personalized permissible financial products and services.

Influenced by the ongoing developments in financial technology, regulatory reforms, and Ghana's expanding digital infrastructure, this Open Banking Directive is a pioneering initiative set to significantly improve Ghana's financial services sector, through the promotion of financial transparency, consumer protection, innovation, trust in the financial ecosystem, and competition among RFIs to improve the overall financial ecosystem experience and ultimately promote a sound and efficient open banking ecosystem.

4.0 Objectives

The objectives of this Open Banking Directive are to:

i. Promote and deepen financial inclusion;

ii. Facilitate the secure sharing of customer-consented data;

iii. Promote innovation in financial service delivery; and

iv. Engender competition among RFIs.

5.0 Scope

The Open Banking Directive is mandatory and shall apply to all RFIs. Data shared shall be on the basis of consent granted explicitly by the Data Subject through established secure and standardized APIs over the designated public digital infrastructure hereby, referred to as OpenDX.

5.1 Participants

The OpenDX shall facilitate the sharing and receiving of customer-consented data among the following participants:

i. Participating Institutions

These shall include payment and financial institutions licensed by the Bank:

a. Universal Banks;
b. Development Banks;
c. Savings and Loans Companies;
d. Micro-Finance Companies;
e. Apex Bank;
f. Rural and Community Banks;
g. DEMIs;
h. PSPs; and
i. PFTSPs.

ii. Any other institution that the Bank may approve and deem as relevant in achieving the objectives of the open banking directive;

iii. Data subjects.

5.2 Data Sets

Data and data sets shall be standardized and accurate for the purpose of providing financial products and services tailored to the needs of Data Subjects. Data Subjects shall provide consent to the sharing of their data before that data is shared. Data to be shared under this Directive shall include:

i. Customer Personal Data**:** Identifiable Data Subject information that can be used for KYC and CDD.
ii. Customer Financial Data: The Data Subject's financial data from financial service providers including account information data, transaction data payments data, and credit data.
iii. Generic services data: Publicly available information including financial product data and market data.
iv. Any other data as determined by the Bank.

6.0 Guiding Principles

For the purpose of fulfilling the objectives, participating institutions shall pursue their activities ethically and responsibly by observing the following guiding principles;

i. **Transparency** – data subjects shall have full knowledge of which participating institutions have access to their data, what data is being shared, how it is being used and for what duration.

ii. **Interoperability** –Data exchange shall be enabled seamlessly across RFIs.

iii. **Usability** – Data shared shall be meaningful, useful, comprehensive and in an acceptable form to the Data Recipient for the purpose of satisfying the needs of the Data Subject.

iv. **Reciprocity** – All Participating institutions shall share data once consent is granted.

v. **Ethical Conduct** – Participating institutions shall conduct themselves according to professional standards.

vi. **Data Quality** – Data shall be accurate, complete, available, usable, and reliable.

vii. **Data Security** - Data shall conform to provisions under the Data Protection Act, 2012 (Act 843) and the Cyber Security Act 2020, (Act 1038) and/or any other applicable data protection or cyber security related laws in force at the time the data is procured.

viii. **Inclusivity** – Participating Institutions shall have access to the data sharing platform (OpenDX) through approved standardized APIs.

ix. **Timeliness** – Participating Institutions shall share and receive consented data in a timely manner.

7.0 Governance

For the purpose of effective and efficient operationalization of the open banking service, the Open Data Exchange (OpenDX) platform, a dedicated public digital infrastructure, shall be established to facilitate the safe and secure sharing of customer-consented data amongst Participating Institutions.

The OpenDX shall be a legal entity, established by the Bank, and governed by a Board of Directors.

7.1 Functions of OpenDX

OpenDX shall among others:

i. Govern API standardization and Regulatory Technical Standards;
ii. Define standardized data formats;
iii. Provide access for Participants to manage consent requests;

iv. Ensure effective management of consent;

v. Ensure encryption of consented Data;

vi. Facilitate secure transmission of Data;

vii. Provide real time notification for consent management; and

viii. Maintain up to date registry of participants.

8.0 Participating Contracts

i. By agreeing to participate in the Open Banking Service, Participating Institutions shall;

a. abide by all provisions outlined in this Directive;

b. acknowledge and commit to securely sharing customer-consented data with each other via OpenDX using approved standardized APIs;

c. comply with all applicable data protection, privacy and AML/CFT/CPF laws in Ghana;

d. accept that any failure to comply with rules and regulations of this Directive could lead to penalties including, but not limited to, exclusion from the Open Banking Service;

e. review and update periodically their compliance procedures to align with any changes to this Directive or relevant laws and regulations;

f. foster healthy competition, stimulate innovation, and contribute towards the development of financial products and services that meet the needs of Data Subjects; and

g. understand that the Open Banking Service demands transparency in all transactions and shall actively work towards building trust with Data Subjects.

ii. This Directive shall be governed by agreements to be entered into by and between the Bank, OpenDX and Participating Institutions. These agreements shall seek to address pertinent issues including:

a) Requirements to be fulfilled to qualify as a Participating Institution;
b) Requirements on data sharing;
c) Requirements to seek consent from Data Subjects; and
d) Requirements and standards for identity verification.

9.0 Access Rules

Participating Institutions shall be required to connect to the FICSOC or have an inhouse Security Operating Centre (SOC) licensed by the Cyber Security Authority (CSA). The following access rules shall apply:

i. Participating institutions shall provide standardized APIs in accordance with OpenDX published standards for use in the sharing of data and services covered by this Directive.
ii. Information sharing shall be allowed only by the presentation of proof of consent by the Data Subject and authentication of such proof as owned by the Data Subject.
iii. The authentication process shall be done via the OpenDX with the data holder to ensure that the prescribed authentication method according to the set standards are always used.
iv. Access to the Data Subject's data shall be based on the Data Subject's explicit and informed consent. Participating institutions shall obtain valid and revocable consent from the Data Subject before accessing their data and must adhere to the customer-granted scope of access.
v. Participating institutions shall implement secure authentication mechanisms to ensure the identity and authorization of customers. Strong customer authentication protocols, such as multi-factor authentication, must be employed to prevent unauthorized access to customer data.

vi. Data transmitted and stored shall be encrypted using industry-standard encryption algorithms to ensure confidentiality, integrity and security of customer data during transmission and storage.

vii. Participating institutions shall maintain comprehensive audit trails to track and monitor access to customer data. The audit trails shall capture relevant information, including the date, time, nature of access, and the identity of the entity accessing the data to assist in detecting and investigating any unauthorized access or potential security breaches.

viii. Data subjects shall have the ability to revoke consent at any time. Participating institutions shall promptly respond to revocation requests and cease accessing and processing customer consented data once consent has been revoked (unless permitted by law).

10.0 Consent Management

This Directive shall be supported by the robust consent management regime below that defines how participants obtain, store, and share consent from data subjects.

i. A Participating Institution shall not process personal data without the prior consent of the Data Subject.

ii. Data Subjects shall be required to register for the Open Banking Service to participate in data sharing.

iii. A Data Subject that gives consent to a Data Recipient authorizes the Data Recipient to collect, process and use the data, received from the Data Holder, for the purposes disclosed by the Data Recipient.

iv. Consent given by a Data Subject to a Participating Institution shall not be considered as a consent to all Participating Institutions. A Data Subject shall give consent to each Participating Institution to retrieve or transmit data.

v. Consent shall be requested from a Data Subject for each data set being shared with a Participating Institution.

vi. The public shall be provided with a verification source to determine the status of their participation.

vii. A Data Recipient shall receive and use consented data for the requested service which is specific, explicitly defined, lawful and related to the permissible activities of that Data Recipient.

viii. A Data Recipient shall disclose to the Data Subject the purpose for the collection of the data.

ix. A Data Subject shall be notified of the time of the transfer of the consented Data.

x. A Data Subject who gives consent to a Data Recipient permits the data to be used by employees and third parties engaged by the Data Recipient in its service delivery.

xi. A Data Recipient that engages the services of a third party for the purpose of delivering services to a Data Subject shall disclose the involvement of the third party to the Data Subject.

10.1 Revocation of Consent

i. A Data Subject can revoke consent at any given time through their RFI to whom they gave consent.

ii. Where a Data Subject revokes consent to share data, the Data Holder shall cease sharing the data with immediate effect.

iii. A Data Subject shall be notified of consent revocation and renewal. The process for revocation of consent by the Data Subject shall be explicitly provided by the RFI. The information shall include;

   a. A statement that the Data Subject can revoke their consent at any time.

b. A simple process for revocation of consent including how already shared data will be treated.

iv. A Data Recipient shall cease to utilize data shared once consent has been revoked by the Data Subject.

v. There shall be no automatic renewal of consent.

vi. Consent shall be valid for a period not exceeding one (1) year, after which a new consent may be granted by the Data Subject.

11.0 Data Privacy and Ethics

A Participating Institution shall:

i. comply with the Data Protection Act, 2012 (Act 843) and any relevant data protection regulation, guidelines, or directives for data protection in Ghana.

ii. consider the privacy of the individual as stipulated in sections 17 and 18 of Act 843 when transmitting data.

iii. Only collect and retain data that is necessary for the provision of agreed-upon services. Any unnecessary data collection or retention is strictly prohibited.

iv. ensure that data is securely transmitted to prevent unauthorized access or data breaches. This includes the use of secure APIs and encryption protocols.

v. put in place secure systems for data storage. This includes protection against both external attacks and internal breaches.

vi. ensure that third party service providers whom consented data is shared with comply with this Directive and all applicable data protection laws and regulations. The Participating Institution is responsible for any data breaches or misuse by these third parties.

12.0 Information Sharing

i. Participating Institutions shall comply with the prescribed standards required for integration;

ii. Data Subjects shall be presented with the information below by the Data Recipient for confirmation and acceptance before consent becomes valid;

   a. Legal and trading name of the Data Recipient and Open Banking Registry identification number of the Data Recipient.
   b. Compliance with access level to data by service category.
   c. The request shall have the following description at minimum;
      1. Service or product that has been requested for.
      2. Duration of the consent before it is invalidated.
      3. Frequency (one-off or multi) of access to consented data set to the Data Recipient.
      4. Where applicable, disclosure of third parties shall be required.

12.1 Enabling data flow

Participating institutions shall:

i. implement APIs according to the standards set by the OpenDX to enable the following:
   a. Submission and authentication of consent.
   b. Verification of consent.

ii. pull & push consented data via standardized APIs.

iii. maintain a log of all information shared.

12.2 Verification Obligation

The Data Holder shall implement authentication procedures and controls. The authentication procedures and controls shall be compatible with the Cyber

Security Act 2020 (Act 1038), the Bank of Ghana's Cyber & Information Security Directive 2018, and any other applicable regulatory directive.

i. A Data Holder shall:
   a. verify the Multi-Factor Authentication (MFA) of the Data Subject to confirm their consent upon receipt of a request.
   b. perform the following when they receive a Data Subject's consent for data sharing with a Data Recipient;
   1. Verify the Data Subject's consent via the approved verification process provided by the OpenDX.
   2. Verify that the request contains the credentials (refer to information in 12.0 (ii)(a))of the Data Recipient.

ii. The Data Recipient shall:
   a. verify that the Data Subject is registered on the OpenDX;
   b. verify that the dataset received is the dataset requested from the Data Holder.

iii. OpenDX Platform shall;
   a. Validate the status of the RFI;
   b. transmit the data request from the Data Recipient and the data requested from the Data Holder;
   c. ensure that the data shared is encrypted during transmission.

13.0 Responsibilities of Parties

The following shall be the responsibilities of the parties under the Open Banking Service:

i. Bank of Ghana.
   The Bank shall:

   a. setup and ensure the seamless operation of the OpenDX platform;

b. appoint competent persons to serve on the Board and Management of the OpenDX;
c. oversee the conduct and operations of Participating Institutions;
d. be the tertiary point of call in respect of consumer complaints left unresolved by Participating Institutions, or with conclusions unsatisfactory to the Data Subjects;
e. educate the public on open banking.

ii. OpenDX

OpenDX shall:

a. coordinate and provide leadership in the creation of the necessary infrastructure for data sharing;
b. determine the standards for APIs and other infrastructure required to connect to the OpenDX;
c. govern API development;
d. provide the terms and conditions for utilizing the OpenDX platform;
e. collaborate with Participating Institutions to define minimum data points.
f. notify Participants about terminations and sanctions, where applicable.

iii. Participating Institutions

The RFIs shall:

a. ensure integrity of data to be shared;
b. ensure security of data shared and received;
c. ensure data is specifically used for the purpose for which it was obtained;
d. ensure consent is given by Data Subject before sharing that data;
e. ensure confidentiality of data shared or received;

f. ensure compliance with legal and regulatory directives governing the Open Banking Service;
g. ensure APIs are maintained and work seamlessly and efficiently;
h. inform Data Subjects on the use of their data;
i. educate employees on the Open Banking Service; and
j. be the first point of call with respect to consumer complaint resolution.

iv. Data Subjects

Data Subjects are advised to:

a. understand the products and/or services the Data Recipients are offering before giving consent to access their data; and
b. read fully and understand all terms and conditions pertaining to the sharing of their data before giving consent to the Participating Institution.

14.0 Liabilities of Parties

The following shall be the liabilities of the parties under the Open Banking Service:

i. OpenDX

OpenDX shall rectify any security breaches with the OpenDX platform.

ii. Participating Institutions

Participating institutions shall be liable for the following:

a. Breach of participating rules set out to govern this Open Banking Service;
b. Data protection breaches as stipulated in the Data Protection Act 2012 (Act 843) and any other regulations, directives and guidelines that may apply;

c. Breaches of data confidentiality and misuse by third parties whose services have been engaged by Participating Institutions in their service delivery to Data Subjects;

d. Fraudulent transactions resulting from data breaches;

15.0 Rights of the Data Subject

i. *Data Ownership*: A Data Subject shall have the right over their data including which type of data can be shared, with whom, and for what purpose(s).

ii. *Data Privacy and Security*: A Data Subject is entitled to data protection. All data sharing under the Open Banking Service shall comply with the applicable privacy laws and data protection standards.

iii. *Informed Consent*: A Data Subject shall be informed about the implications of data sharing before they give consent. This includes understanding which data will be shared, how it will be used, and how it will be protected.

iv. *Revocation of Consent*: A Data Subject can revoke consent to share data at any time. Upon revocation, no further data shall be transferred or used.

v. *Access to Services*: A Data Subject shall have the right to participate in the Open Banking Service and shall not be denied based on their decision to share or not to share their data with specific Participating Institutions.

vi. *Redress*: A Data Subject shall have the right to lodge complaints against a Participating Institution if they believe their rights have been infringed. They shall have access to fair dispute resolution procedures in line with the Consumer Recourse Mechanism Guidelines 2017.

16.0 Anti-Money Laundering and Countering the Financing of Terrorism and Combating Proliferation Financing (AML/CFT/CPF)

Participating Institutions shall comply with the Anti-Money Laundering Act, 2020 (Act 1044), regulations, guidelines, directives, and notices on Anti-Money Laundering, Countering the Financing of Terrorism and Combating Proliferation Financing.

Participating Institutions shall conduct a risk assessment on new technologies and comply with provisions in Act 1044 on reliance on third parties and customer due diligence measures.

17.0 Reporting Requirements

Participating Institutions shall submit periodic reports as may be determined by the Bank on the following:

i. Number of Data Subjects;

ii. Logs of data shared and data received for the period;

iii. Incident logs and resolution for the period;

iv. Downtime reports and its impact;

v. Fraud incidents;

vi. API performance levels; and

vii. Any other requirements as may be determined by the Bank.

18.0 Cybersecurity Breach Incident Reporting

Participating Institutions shall ensure the following preventive data security measures are implemented to safeguard the Open Banking ecosystem:

i. A robust incident reporting mechanism and procedure shall be put in place to ensure the timely detection, response, and mitigation of cybersecurity breaches.

ii. Report any security incidents and/or breaches, within twenty-four hours, to OpenDX to ensure effective response, investigation, and mitigation of potential risks.

iii. Cybersecurity breach incident reporting shall cover the following key areas:

a) Incident Classification and Severity Levels;
b) Internal Incident Reporting Channels;
c) Reporting Timelines and Escalation Procedures;
d) Incident Investigation and Documentation;
e) Incident Response and Mitigation; and
f) Regulatory Reporting and Compliance.

19.0 Data Breach Policy and Procedure

Upon detection of a data breach by a Participating Institution;

i. the Incident Response Team (IRT) shall take actions to contain the breach, prevent further escalation and mitigate potential damage.

ii. the Participating Institution shall report the suspected or confirmed data breach to OpenDX.

19.1 Data Incident Management Procedure

i. Data Monitoring and Logging

Participating Institutions shall:

a. continuously monitor systems, networks, and applications for suspicious activities and potential security breaches;

b. collect and analyze logs to detect anomalies and unauthorized access attempts.

ii. Vulnerability Assessment

a) A Participating Institution shall ensure that they conduct their annual Vulnerability Assessment and Penetration Test (VAPT) on every critical infrastructure holding and/or processing customer data to identify and remediate vulnerabilities in the infrastructure. Participation in the Open Banking Service is contingent on submitting an annual VAPT report to OpenDX as required by the Cyber and Information Security Directive, 2018.

iii. Data Breach Response

Upon detection of a data breach by a Participating Institution;

a) The designated IRT shall conduct an initial assessment to determine the nature, scope, and potential impact of the incident;
b) The incident shall be categorized based on its severity and potential impact, ranging from low-risk incidents to high-impact breaches;
c) The IRT shall promptly take actions to contain the breach, prevent further escalation and mitigate potential damage;
d) Evidence related to the breach shall be preserved, as prescribed in Act 987;
e) The designated IRT shall investigate the breach to identify the root cause of the breach and implement corrective measures to prevent future occurrence;
f) All incident details, response actions, and communications shall be documented for analysis and reporting purposes;

iv. Data Breach Reporting

a. A Participating Institution shall report the attempted or successful data breach to OpenDX. The report shall include:

1. The nature of the data that was breached;
2. The number of Data Subjects affected by the breach; and

3. The potential impact of the breach on the Data Subjects' privacy.

a) A Participating Institution shall notify affected Data Subjects of the breach in a clear and timely manner, providing relevant information and guidance on protective measures.

b) A Participating Institution shall provide timely complaint notification to relevant data protection authorities as required by the Data Protection Act, 2012 (Act 843) and other applicable laws and regulations.

20.0 Risk Management

A Participating Institution shall:

i. incorporate into its enterprise risk management framework, identified risks and mitigating controls associated with Open Banking in compliance with relevant and applicable laws, regulations and directives.

ii. have a risk assessment framework relating to Open Banking which will be submitted to OpenDX for assessment before they are permitted to participate.

20.1 Risk Management Committee

Participating Institutions shall establish a risk management committee, if they have not already established one, which shall consist of at least two (2) members of senior management including senior managers responsible for compliance and information security or their equivalent designations in an institution. Their responsibilities shall include:

i. exercising oversight of relevant documented controls, and security measures for business operation systems, networks, data centres and operations backup facilities associated with its participation in the Open Banking Service;

ii. preparation and submission of risk management reports associated with its participation in the Open Banking Service to the Board.

20.2 Risk Management Reporting

The following shall apply for risk management reporting for Participating Institutions:

i. A risk management reporting procedure shall be established to provide the OpenDX, on a regular basis, with an updated assessment of security risks and the measures taken by Participating Institutions in protecting customer-consented data to ensure safety and soundness of the Open Banking Service;
ii. Application for authorisation to participate in the Open Banking Service shall be accompanied by a description of the procedure to monitor, handle and follow up on security incident and security-related customer complaints, including incident reporting mechanism.

21.0 Sanctions and Penalties

Any action which contravenes any section of this Directive shall attract the corresponding sanctions and penalties under the applicable laws.

22.0 Termination and suspension

The Bank reserves the right to suspend or terminate the Participating Institution's access to the Open Banking platform in cases of non-compliance with the terms and conditions stipulated in this Directive.

22.1 Suspension

i. In the event of non-compliance to any provision in this Directive, the Bank shall suspend the Participating Institution's access to the OpenDX platform.
ii. A suspended Participating Institution shall submit to the Bank a comprehensive corrective action plan prior to rectifying the non-compliance.
iii. The suspension shall remain in effect until the Participating Institution rectifies the non-compliance to the satisfaction of the Bank.

22.2 Termination

i. If the Participating Institution fails to rectify the non-compliance within a stipulated period or in cases of recurrent non-compliance, the OpenDX may terminate the Participating Institution's participation in the Open Banking Service. A termination notice will be issued, and the Participating Institution will be obliged to cease all activities in the Open Banking Service immediately.
ii. The Bank reserves the right to direct OpenDX to terminate the Participating Institution's access in cases of insolvency, liquidation, or cessation of business activities of the Participating Institution.
iii. The Bank or OpenDX may terminate participation of an RFI if deemed necessary to protect the integrity of the financial ecosystem or the interests of Data Subjects.
iv. Any suspension or termination under this clause does not preclude the Bank, OpenDX or a Participating Institution from taking other regulatory or legal action against a Participating Institution.
v. Participating Institutions may petition the Bank for redress where it is not satisfied with the decision of OpenDX.

23.0 Dispute Resolution

i. Participating Institutions shall have a dispute resolution clause in its contract with the Data Subject in line with the Bank's Consumer Recourse Mechanism Guidelines 2017.

ii. Disputes between Participating Institutions shall be resolved as specified in their Participating Contracts.

iii. Disputes between Participating Institutions and OpenDX shall be resolved as specified in their Participating Contracts.

24.0 Complaint Handling Procedure

i. Participating Institutions shall review their recourse procedures to ensure provisions and mechanisms are in place to handle complaints and inquiries associated with the Open Banking Service.

ii. The recourse mechanism shall be in line with the Bank's Consumer Recourse Mechanism Guidelines for Financial Service Providers February, 2017

iii. Any unresolved disputes shall be escalated to OpenDX and if unresolved, to the Bank.

Definition of Terms

Accounts: Accounts refers to accounts held with applicable RFIs, including wallets.

Account Information: This shall include Data related to customer accounts, such as balances, transaction history, account details, and account ownership information. This is fundamental data which enables services such as account aggregation, personal finance management, and payment initiation.

Application Programming Interface (API): A software that facilitates communication between different applications. The API enables the sharing of data between entities under open banking practice.

Consented Data: The explicit consent given by Data Subjects to share their financial data with financial institutions an. It includes details such as the scope of access, duration of consent, and any specific restrictions or revocations made by the Data Subject.

Credit Data: Credit data consists of information related to customer credit history, credit scores, loan accounts, and repayment behavior. Essential to facilitate the secure sharing of credit data with authorized third-party providers to enable credit scoring, loan comparisons, and access to tailored financial products.

Customer Personal Data: Identifiable customer information that can be used for KYC and customer due diligence.

Customer Transaction Data: Data from a customer's financial service providers that shows the history of transactions including account information data and transaction Data.

Data: Information about participants engaged in the Open Banking Service.

Data Holder: An entity that holds and processes the Data Subject's data in order to transfer the data to a Data Recipient at the Data Subject's request.

Data Recipient: An entity that receives data from a Data Holder at the Data Subject's request to develop products and services for the Data Subject.

Dataset: Categorised data for the purpose of the Open Banking Service.

Data Subject: An individual or company that creates data, owns the data and gives permission for that data to be shared with financial institutions or third-party providers. They are also the end users of products and services developed.

Financial Product Data: Financial product data covers information about various financial products offered by banks and financial institutions. This includes details about interest rates, fees, terms and conditions, eligibility criteria, and other product-specific information.

Generic Services Data: This can be referred to as publicly available information on price, product, agents and branches of financial service providers as well as industry insights including financial product data and market Data.

Market Data: Market data includes real-time or historical financial market information, such as stock prices, exchange rates, and market indices. This data set enables the development of innovative applications and services, such as investment portfolios, financial analytics, and automated trading systems.

Open Banking Service: A policy directive in which Participating Institutions share financial product data and/or certain specific customer data with other Participating Institutions. The sharing of specific customer data is based on request by, and consent of, the Data Subject.

Participating Institutions: Institutions permitted by this Directive to engage in Open Banking Service.

Regulated Financial Institutions: Financial Institutions regulated by the Bank of Ghana and any other institution that the Bank may approve and deem as relevant in achieving the objectives of the open banking directive.

Third-party Providers: Entities that provide services to participating institutions.

Transaction Data: Transaction data encompasses details of individual financial transactions, such as the date, amount, description, and parties involved.