

Privacy Policy

1. Introduction/Scope

This document is prepared in accordance with the provisions of the Ghana Data Protection Act, 2012 (Act 843), and, by extension, the EU General Data Protection Regulation (GDPR). It sets out how Zenith Bank (Ghana) Limited applies and complies with the data privacy principles in processing the personal data of customers, staff, vendors, visitors, and even third parties that interact with the bank.

For personal data of individuals, this document also highlights their rights and covers the data subject(s) whose personal data is collected and processed, in compliance with the DPA.

This privacy policy describes why and how we collect and use personal information about our customers, clients, vendors, and visitors (data subjects). It also highlights with whom we might share personal information and how long we keep it. It also makes data subjects aware of their rights under the regulation.

2. Roles/Responsibilities

The Data Controller and the Designated Data Controllers.

Zenith Bank (Ghana) Limited is the data controller and its executive management is ultimately responsible for implementation.

Zenith Bank's Data Protection Supervisor (DPS) is responsible for ensuring the accuracy of this document and that it is up to date. The DPS also ensures that data subjects are duly notified prior to the collection and processing of their personal data by the bank, including data collected via Zenith Bank Ghana's website. All employees and staff of the bank who interact with personal data must also follow the provisions in this policy document.

3. Policy Statement

Zenith Bank is committed to protecting the privacy and security of our personal data. We are responsible for determining how we hold and use personal information about our data subjects. According to the Ghana Data Protection Act (DPA), Zenith Bank (Ghana) Ltd. must notify data subjects of the information contained in this document.

3.1 About Zenith Bank (Ghana) Ltd.

Zenith Bank (Ghana) Limited, a subsidiary of Zenith Bank Plc, was incorporated in April 2005 under the Companies Code, 1963 (Act 179) as a private limited liability company and licenced by the Bank of Ghana in September 2005 under the Banking Act, 2004 (Act 673) as amended by the Banking (Amendment) Act, 2007 (Act 738) to provide financial services under a Universal Banking Licence.

Since its inception, the Zenith brand has been synonymous with a cutting-edge ICT platform, first class banking products and services that meet customers’ financial needs, passionately innovative staff, and a commitment to exceptional customer service delivery.

The Bank’s service delivery channels include forty-three (43) business locations (branches and agencies), numerous ATMs and Point of Sales terminals strategically located in various cities and towns across Ghana. The bank also offers mobile and internet banking services which enable customers to access banking services on-the-go.

Due to the nature of the Bank’s business and its provision of financial services across the globe, the bank is mandated to collect and process personal data of Ghanaian individuals, as well as residents and citizens of other countries across the globe.

3.2 What Personal Data Do We Need?

The personal data we would collect and process, depending on the particular processing requirement, falls under the following categories:

Data Type	Description of Data
Identity Data	Full Name, maiden name, marital status, title, date of birth, gender, address, employment history and citizenship.
Contact Data	Address, Email Address and Telephone Numbers. Information received during contact through face-to-face meetings, phone calls, emails, letters, and SMS.
Financial Data	Bank account information and bank statements, income and expenditure, financial position, status, and credit history, debit or credit card information and account number.
Transaction Data	Information regarding the products and services a data subject may have benefited from by using Zenith Bank (Ghana) Limited

, transactional information in respect of products purchased.

Location data of transactions where a data subject may have used their debit card.

Technical Data

Internet protocol (IP) address, login data, details of browser and operating system, time zone setting and location, browser plug-in types and versions, platforms, and other technology such as device ID, geolocation, IP, model, and user agent on the devices used to access the Bank's website.

Profile Data

Includes username and password.

Job Application Data

Data submitted throughout the recruitment process e.g. name, email address. Any personal information you provide to Zenith Bank (Ghana) Limited as part of the recruitment process.

Usage Data

Includes information about how data subject uses our website, products, and services

Marketing and Communications Data

Information about data subject communications with the Bank.

Preferences in receiving marketing e-mails and consents given by data subject to the Bank.

Where the personal data we need to collect falls under a special category of sensitive personal data, the bank's lawful basis of processing will be the explicit consent of the individual, or, where applicable, compliance with a legal obligation, or for legal proceedings/advice.

4. Why We Need the Data

Zenith Bank ensures that the personal data collected and processed is necessary for collection and shall not collect or process more data than is reasonably required for a particular processing activity.

5. Legal Grounds for Processing

Zenith Bank identifies, establishes, defines, and documents the specific purpose of processing and the legal basis for processing personal data (including any special categories of personal data processed) before any processing operation takes place under:

- Consent obtained from the data subject.
- Performance of a contract where the data subject is a party.
- Legal obligation that the bank is required to meet.
- Protect the vital interests of the data subject, including the protection of rights and freedoms of the data subject.
- Official authority of the bank or to carry out the processing that is in the public interest.
- National law, such as biometric data.

In addition, every processing purpose has at least one lawful basis for processing to safeguard the rights of the data subjects, as listed below:

Purpose of Processing	Lawful Basis of Processing
Account creation, identity verification and maintenance of records	Contract
Vendor validation/information processing	Contract
Employment	Contract

6. Processing of Personal Data Based on Consent

Where applicable, Zenith Bank will require the explicit consent of customers, visitors, and other relevant stakeholders to process collected personal data.

Visitors to the Bank’s website are expected to read and understand the website privacy notice and then agree to the website’s terms of use. By consenting to the privacy policy, data subjects are permitting Zenith Bank to use or process their personal data specifically for the purpose identified before collection.

On this ground, if any data subject (customer, client, visitor, vendor, staff, or third party) does not agree to Zenith Bank collecting and processing their personal data, such individual is not allowed to enjoy the bank's service(s) where applicable.

If, for any reason, the bank is requesting sensitive personal data from its stakeholders (external and internal), the individuals will be rightly notified of why and how the information will be used.

To ensure the confidentiality and security of personal information, Zenith bank has implemented industry-standard encryption protocols during the transmission, processing, and storage of such data. This includes both at-rest and in-transit encryption methods to safeguard against unauthorized access or disclosure.

Where processing relates to a child under 18 years old, as in the case of DPA, or 16 years old in the case of GDPR, Zenith Bank shall demonstrate that consent has been provided by the person who holds parental responsibility over the child. Zenith Bank shall demonstrate that reasonable efforts have been made to verify the age of the child and establish the authenticity of the parental responsibility, taking into consideration available technology.

You can find more information about how we process personal information by referring to the supplementary privacy notices for particular services.

6.1 Withdrawal of Consent

Irrespective of the initial consent given, an individual can withdraw their consent at any time by making a withdrawal of consent request.

Zenith Bank demonstrates the data subject (customer, client, visitor, vendor, staff, or third-party) has withdrawn consent to the processing of his or her personal data with written instruction from the data subject.

For child consent, Zenith Bank shall demonstrate that the holder of parental responsibility over the specified child has withdrawn consent via written instruction from the parent. The bank will also demonstrate that reasonable efforts have been made to establish authenticity of the parental responsibility when withdrawing consent for the specified child, considering available technology.

Where applicable, the Data Protection Supervisor (DPS) will inform the relevant process owner of this change, and the processing activities that relied upon the consent will be stopped immediately, in accordance with the relevant process.

7. Use of Cookies

The bank's website also uses cookies provided by trusted third parties, such as Google Analytics, to help us understand and improve users' experience on the website.

Zenith Bank may use the information obtained from the use of our cookies to:

- Recognize a computer when a user visits the Bank's website.
- Track whoever navigates the website
- Improve the website's usability (including Live Chat application to answer questions a user may have in real time
- Analyse the use of its website, such as how many people visit it each day, and
- Manage the website.

Users can disable cookies and prevent the setting of cookies by adjusting the settings on their browser. However, this is not recommended, as disabling cookies may also disable certain functionality and features of the site.

8. Disclosure to Third Parties

Aside from situations where the bank may be required to disclose the personal data of individuals in accordance with a legal obligation in response to requests by government authorities or law courts on matters involving national security or law enforcement requirements, Zenith Bank will not pass on its data subjects' personal data to third parties without first obtaining consent.

In situations where the processing of personal data will involve an investigation of potential violations of the bank's terms of service, fraud prevention and mitigation, security issue management, and the preservation of the rights and freedoms of staff, customers, and clients, the bank shall establish an appropriate legal ground for such data transfers.

Zenith Bank has put in place, to the best of its ability and in line with standard global practices, physical, technical, and organizational measures (including secure encryption and anonymization) to ensure the optimum protection of personal data, which also extends to data transferred or shared with third parties.

8.1 Cross-Border Transfers

Zenith Bank may also engage third parties abroad (such as other Banks, contractors, government-authorized agencies, etc.) that will receive personal data for a certain purpose(s) as part of the bank's processing activities and process it on the bank's behalf. Where this is the case, the bank will enter into a data processing agreement with the third party, ask for consent if the purpose of processing was not initially stated at the inception, and be satisfied that the third party has adequate measures in place to protect the data against accidental or unauthorized access, use, disclosure, loss, or destruction.

In a case where the disclosure is to third parties outside the jurisdiction of the DPA, Zenith Bank will ensure that the third party meets the core global regulatory standards before the

transfer. This may include transferring the personal data to a third party where the bank is satisfied that:

- The country of the recipient has adequate data protection controls established by legal or self-regulatory regimes. However, in a case not covered by an adequacy decision from the DPC,
 1. It has a contract in place that uses existing data protection clauses with the approval of DPC to ensure adequate protection.
 2. It is making the transfer under approved binding corporate rules.
- Provisions inserted into administrative arrangements between public authorities or bodies authorised by the supervisory authority DPC.

9. Retention of Records

Zenith Bank stores a broad spectrum of personal information. All information Zenith Bank holds is stored and retained or stored and destroyed in compliance with DPA's guidelines on the retention of records and personal data.

Zenith Bank will retain your personal data as long as the information is active on the bank's systems and necessary for the bank's service delivery purposes. This retention period is verified and established with special consideration to the following areas:

- The requirements of the bank
- The type of personal data
- The purpose of processing
- Lawful basis for processing
- The categories of data subjects

As a regulated financial services institution, the bank will retain your personal data for ten (10) years after the exit of the relationship by the data subject, or as may be required by regulation. When the personal data is no longer needed or beyond the stipulated retention period, Zenith Bank will delete or destroy it from its systems and records or take steps to securely archive it while protecting your identity and privacy rights.

10. Data Subject Rights

At any point while Zenith Bank is in possession of or processing personal data, the data subject has the right to:

- Request a copy of the information that the bank holds about them.
- Correct the data that is inaccurate or incomplete.
- Restrict processing of their personal data where certain conditions apply.
- Have their data transferred to another organisation.
- Object to certain types of processing like direct marketing.
- Object to automated processing like profiling, as well as the right to be subject to the legal effects of automated processing or profiling.
- Complain and pursue judicial review in the event that the Bank refuses their request under rights of access without a clear and justifiable reason.

All the above requests will be forwarded should there be a third party involved in the processing of your personal data.

11. Complaints

If for any reason a vendor or contractor, customer, or staff member wishes to make a complaint about how Zenith Bank (or any of the Bank's third parties) handles or has handled their personal data, or how their complaint has been handled, they have the right to complain directly with;

- the supervisory authority

NAME	<i>Data Protection Commission</i>
ADDRESS	<i>East Legon, Pawpaw Street, (GA-414-1469), Accra P.O. Box CT 7195, Accra</i>
TELEPHONE	<i>+233256301533</i>
EMAIL	<i>info@dataprotection.org.gh</i>

- and Zenith Bank

NAME	<i>Zenith Bank Data Protection Supervisor</i>
ADDRESS	<i>Zenith Heights, No. 37 independence Avenue (GA-030-7585), Accra P.M.B. CT 393, Accra</i>
TELEPHONE	<i>0302660421 / 0531100068</i>
EMAIL	<i>Dataprotectionsupervisor@zenithbank.com.gh</i>

12. Changes to Privacy Notice

We are constantly trying to improve our website and services, so we may need to change this privacy notice from time to time as well. We will alert you to material changes by, for example, placing a notice on our websites and/or by sending you an email (if you have registered your e-mail details with us) when we are required to do so by applicable law.