ABC FINANCE CORPORATION

DATA PRIVACY MANUAL (DPM)

2024 VERSION

I. BACKGROUND

Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), aims to protect personal data in information and communications systems both in the government and the private sector. The DPA created the National Privacy Commission (NPC) which is tasked to monitor its implementation. It covers the processing of personal information and sensitive personal information and sets, as its basic premise, the grant of direct consent by a data subject before data processing of personal information is allowed.

The law requires all government and private entities or organizations processing personal data to establish policies and implement measures and procedures to ensure and guarantee the safety and security of personal data under their control or custody, thereby upholding an individual's data privacy rights. In addition, they are required to implement reasonable and appropriate measures to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination.

To inform its personnel and data subjects of such measures, all agencies are expected to produce a DPM. The DPM serves as a guide or handbook for ensuring the compliance of an organization or entity with the DPA, its Implementing Rules and Regulations (IRR), and other relevant issuances of the NPC. It also encapsulates the privacy and data protection protocols that need to be observed and carried out within the organization for specific circumstances (e.g., from collection to destruction), directed toward the fulfillment and realization of the rights of the data subjects.

II. INTRODUCTION

The ABC Finance Corporation ("Corporation"), in its commitment to uphold, respect, and value data privacy rights hereby adopts this DPM in compliance with the DPA, its IRR, and other relevant policies, including issuances of the NPC.

The Corporation ensures that through this DPM all personal data collected from all its clients and other data subjects shall be processed in adherence to the general principles of transparency, legitimate purpose, and proportionality. To guide the Corporation and its data subjects in exercising their rights under the DPA, this DPM shall include data protection and security measures.

III. DEFINITION OF TERMS

Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic, or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.

Data subject refers to an individual whose personal information is processed.

Filing system refers to any act of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular person is readily accessible.

Information and Communications System refers to a system for generating, sending, receiving, storing, or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or which data is recorded, transmitted, or stored and any procedure related to the recording, transmission or storage of electronic data, electronic message, or electronic document.

Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

Personal information controller refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes a person or organization who performs such functions as instructed by another person or organization; and an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

Personal information processor refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

Privileged information refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.

Sensitive personal information refers to personal information about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and specifically established by an executive order or an act of Congress to be kept classified.

IV. SCOPE AND LIMITATIONS

This DPM is hereby adopted in compliance with Republic Act No. 10173 or the DPA of 2012, its IRR, and other relevant policies, including issuances of the NPC.

This DPM applies to all departments and units within the Corporation, all employees and third-party service providers who handle personal data on behalf of the Corporation, and all types of personal data processed by the Corporation, including customer, employee, supplier, and partner data.

While this DPM aims to provide comprehensive guidance on data privacy practices, it does not cover personal data processing activities conducted outside the scope of the Corporation's operations, data processed by third-party entities that are not directly engaged by the Corporation, and any data processing activities governed by different jurisdictions not explicitly covered in this DPM.

Furthermore, this DPM does not provide detailed instructions for every specific data privacy scenario but outlines general principles and procedures to be followed. Employees and stakeholders are encouraged to seek additional guidance from the Data Protection Officer (DPO) or the Legal Department when dealing with unique or complex data privacy issues.

V. PROCESSING OF PERSONAL DATA

1. Collection

The Corporation collects personal data from clients to provide services. This data includes full name, address, and cellular/telephone numbers. These are obtained openly and straightforwardly without any hidden motive through the clients filling out the Corporation's forms. The collection of both personal information and sensitive personal information is done by lawful means and for a lawful purpose.

2. Processing or Use

Personal data collected from clients will be used to deliver services, process transactions, and communicate with clients about their inquiries. The Corporation shall ensure no manipulation of personal data and that the same shall not be used against any client.

3. Storage, Retention and Destruction

The Corporation shall ensure that personal data under its custody are protected against any accidental or unlawful destruction, alteration, and disclosure as well as against any other unlawful processing.

Client data will be stored in secure databases with access restricted to authorized personnel only and retained for five (5) years after the last interaction with the client. After said period, all hard and soft copies of personal information shall be disposed of and destroyed through industry-standard methods.

4. Access

Access to personal data is granted only to authorized personnel based on their roles and responsibilities. At no time should anyone be given access to the personal files of other employees.

For the personal data of clients, only the DPO, Internal Auditor, Chief Technology Officer, and the managers and staff of the Processing Department shall have access to the same.

5. Disclosure and Sharing

All employees of the Corporation shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after resignation, termination of contract, or other contractual relations.

Personal data under the custody of the Corporation shall be disclosed only for a lawful purpose and authorized recipients of such data.

VI. SECURITY MEASURES

A. Organization Security Measures

a. Data Protection Officer (DPO) or Compliance Officer for Privacy (COP)

The Compliance Manager and Compliance Officers are designated Data Protection Officers.

b. Functions of the DPO, COP, and/or any other responsible personnel with similar functions

1. Monitor the Personal Information Controller's (PIC) or Personal Information Processor's (PIP) compliance with the DPA, its IRR, issuances by the NPC, and other applicable laws and policies. As such he/she may:

a. Collect information to identify the processing operations, activities, or systems of the PIC or PIP, and maintain a record thereof;

b. Analyze and check the compliance of processing activities and compliance by third-party service providers;

c. Inform, advise, and issue recommendations to the PIC or PIP;
d. Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
e. Advice the PIC or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law;

2. Ensure the conduct of Privacy Impact Assessments relative to activities or systems of the PIC or PIP;

3. Advise the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights such as requests for information, clarifications, rectification, or deletion of personal data;

4. Ensure proper data breach and security incident management by the PIC or PIP, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;

5. Inform and cultivate awareness of privacy and data protection within your organization, including all relevant laws, rules, regulations and issuances of the NPC;

6. Advocate for the development, review, and/or revision of policies, guidelines, projects, and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy-by-design approach;

7. Serve as the contact person of the PIC or PIP vis-à-vis data subjects, the NPC, and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP;

8. Cooperate, coordinate, and seek advice from the NPC regarding matters concerning data privacy and security; and

9. Perform other duties and tasks that may be assigned by the PIC or PIP that will further the interest in data privacy and security and uphold the rights of the data subjects.

c. Conduct of trainings or seminars to keep personnel, especially the Data Protection Officer updated vis-à-vis developments in data privacy and security

The Corporation shall sponsor mandatory training on data privacy and security at least once a year. This covers best practices in the protection of personal data, handling sensitive data, and recognizing phishing attempts or unlawful access.

d. Conduct of Privacy Impact Assessment (PIA)

The Corporation shall conduct a PIA relative to all activities and systems involving the processing of personal data.

The Corporation may opt to outsource the conduct of a PIA provided that before engaging with a third-party service provider, the former will assess the security protocols and require the latter to sign data protection agreements.

e. Recording and documentation of activities carried out by the DPO, or the organization itself, to ensure compliance with the DPA, its IRR and other relevant policies.

It is imperative for employees who have direct access to personal data to ensure they regularly attend and actively participate in relevant training sessions and orientations about DPA.

f. Duty of Confidentiality

A Non-Disclosure Agreement will be required to be signed by each employee.

All employees who have access to personal information are required to keep it strictly confidential if it is not meant for public disclosure.

g. Review of Privacy Manual

This DPM shall be reviewed and evaluated annually.

The Corporation will update its privacy and security policies and procedures to stay compliant with best practices for data privacy.

B. Physical Security Measures

1. Format of data to be collected

Personal data in the custody of the Corporation may be in digital/electronic format and paper-based/physical format.

2. Storage type and location

Physical documents containing personal data are stored in locked cabinets, and shredders are used to dispose of sensitive documents securely.

Digital /electronic files shall be stored in computers protected by passwords and can be accessed only by authorized personnel.

3. Access procedure of agency personnel

Data processing facilities are secured with access controls such as key card entry, security personnel, and surveillance cameras.

4. Monitoring and limitation of access to room or facility

The Corporation uses CCTV cameras to monitor entry points, data storage areas, and other critical locations. Security footage is regularly monitored and reviewed to detect any suspicious activity or security breaches.

All authorized personnel who accessed the stored personal data must fill out and register access details in a logbook and/or the Corporation's workplace system. They shall indicate the date, time, duration, and purposes of each access.

5. Design of office space/workstation

All workstations accessing personal data are locked when not in use and are protected with strong passwords.

Our server rooms are equipped with fire suppression measures, temperature sensors, and humidity control to prevent damage to servers and data.

6. Persons involved in processing, and their duties and responsibilities

Every employee who processes data is required to constantly protect the integrity and confidentiality of such data.

7. Modes of transfer of personal data within the organization, or to third parties

Emails containing personal information must be sent through a secure email provider that encrypts the content, including any attachments. Further, the Corporation uses the warning message features in Google Business.

8. Retention and disposal procedure

Client information will be kept for five (5) years from the conclusion of the client's final engagement and kept in safe databases to which only authorized people have access. When disposing of old hard drives, the Corporation follows a strict procedure that includes data wiping using certified software. Paper documents are shredded on-site.

C. Technical Security Measures

a. Monitoring for security breaches

The Corporation shall procure and install anti-virus software, on an annual basis, for devices that regularly access the internet. The Chief Technology Officer (CTO) shall regularly read the firewall logs to monitor security breaches and alert the Management of any unauthorized attempt to access the Corporation’s network.

b. Security features of the software/s and application/s used

The CTO shall first review and evaluate software applications before the deployment thereof in computers and devices of the Corporation to ensure compatibility of security features with the data privacy policies.

On existing software applications, that involve the processing of personal data of clients and employees, the end user, with the technical assistance of the CTO, shall evaluate and assess the security protocols of the system concerning saving, backup, and data recovery. If such protocol runs counter to the data privacy principles stated in the DPA of 2012, corrective action should be taken to address the issues.

c. Process for regularly testing, assessment and evaluation of effectiveness of security measures

The CTO and his team perform weekly vulnerability scans and penetration testing of the firewall to proactively address security vulnerabilities against viruses and hackers.

d. Encryption, authentication process, and other technical security measures that control and limit access to personal data

The Corporation employs strong encryption for data transmitted over its network. Additionally, personal data stored in the databases is encrypted using industry-standard algorithms. Access to the Corporation's systems containing personal data requires individual user authentication. The Corporation enforces strong password policies and regularly reviews access permissions.

VII. BREACH AND SECURITY INCIDENTS

1. Creation of a Data Breach Response Team

   A Data Breach Response Team (DBRT) comprising the CTO and DPO is responsible for ensuring immediate action in the event of a security incident or personal data breach. Upon receiving a report, the DBRT conducts a thorough investigation wherein they will assess the scope of the incident, evaluate potential risks, and determine whether it qualifies as a data breach under applicable regulations.

2. Measures to prevent and minimize occurrence of breach and security incidents

   The Data Breach Response Team shall regularly conduct a Privacy Impact Assessment to identify risks in the processing system and monitor for security breaches and vulnerability scanning of computer networks. The CCTV Footage is regularly reviewed for security purposes.

3. Procedure for recovery and restoration of personal data

   The Corporation maintains off-site backups in a secure facility. Further, the Corporation regularly tests and verifies data restoration processes and has real-time monitoring in place to detect unauthorized access or suspicious activities.

4. Notification protocol

   The Head of the DBRT shall inform the Corporation's Board of Directors of the need to notify the NPC and the data subjects affected by the incident or breach within 72 hours of knowledge thereof.

5. Documentation and reporting procedure of security incidents or a personal data breach

   The Corporation keeps thorough records of every security incident or breach of personal data. It also keeps an annual report of security incidents or breaches of personal data, which must be submitted to the Corporation's Management and NPC within the time frame specified by law and/or NPC's circular.

The report shall contain the description of the nature of the breach; personal data possibly involved; measures undertaken by the team to address the breach and reduce the harm or its negative consequences; and names of the personal information controller, including contact details, from whom the data subject can obtain additional information about the breach and any assistance to be provided to the affected data subjects.

VIII. INQUIRIES AND COMPLAINTS

For inquiries or complaints about data privacy, please contact our Data Protection Officer at dataprotection@abcfinance.ph or call our dedicated privacy hotline at 09171071642.

The Corporation aims to acknowledge inquiries within 48 hours and provide a substantive response within 10 business days. Upon receiving a complaint, our DPO initiates an investigation. The Corporation communicates with the complainant, addresses their concerns, and takes necessary corrective actions.

If an individual is dissatisfied with the corporation's response, they have the right to escalate the matter to the relevant data protection authority. Complaints shall be filed in three printed copies, or sent to the department concerned and the latter shall confirm with the complainant its receipt of the complaint. The Corporation provides guidance on this process and in addition to inquiries and complaints, individuals can also request to exercise their privacy rights. The Corporation's DPO will assist with such requests.

IX. EFFECTIVITY

The provisions of this DPM are effective this 1st day of July 2024, until revoked or amended by the Corporation, through a Board Resolution.

X. ANNEXES

1. Consent Form

Borrower's Consent

JOINT CONSENT
Form

I/We, _____, have read ABC FINANCE CORPORATION Data Privacy Statement in connection with RA 9510 (Credit Information System Act) and RA 10173 (Data Privacy Act) and their respective implementing rules and regulations as well as other laws and issuances and express our consents for ABC FINANCE CORPORATION to collect, record, organize, update or modify, retrieve, consult, use, consolidate, block, erase or destruct my personal data as part of my information.

I/We and/or my/our authorized representative hereby consent (if customer cannot sign) to the processing and disclosure of the customer's information by ABC FINANCE CORPORATION its representative which is necessary for the approval and/or collection of my loan.

I/We, as principal borrower, co-maker/s and guarantor/s authorize ABC FINANCE CORPORATION or its representatives through this Joint Consent to disclose the data of the principal borrower, co-maker/s, guarantor/s and all other information relative to the loan I/ we have with ABC FINANCE CORPORATION either as principal borrower, co-maker/s and/or guarantor/s to one another or to our respective spouses or to our natural or adopted brothers or sisters or to our ascendants or descendants within the 4th civil degree by blood or affinity.

My/Our withholding or withdrawal of such consent shall relieve ABC FINANCE CORPORATION, its owners, directors, officers, employees and representatives from any obligation/s to deliver the appropriate service to me as their customer.

We declare that we and/or our authorized representative have full capacity and/or authority to sign and further acknowledge that we are appraised of our rights and protection in accordance with RA 9510 (Credit Information System Act) and RA 10173 (Data Privacy Act) and their respective implementing rules and regulations as well as other laws and issuances. Furthermore, we hereby affirm our rights to be informed, object to processing, access and rectify, suspend or withdraw my personal data and be indemnified in case of damages pursuant to the provisions of RA 9510 (Credit Information System Act) and RA 10173 (Data Privacy Act) and their respective implementing rules and regulations as well as other laws and issuances.

Signature Over Printed Name

Signature Over Printed Name

Signature Over Printed Name

Signature Over Printed Name

2. Inquiry Summary Form

Customer Inquiry Form

Customer Information

- **Name:** _____
- **Email Address:** _____
- **Contact Number:** _____

Service Information

- **Service of Interest:** _____
- **Inquiry Type:** _____
- **Preferred Response Method: () Email () Phone () In-Person Meeting**

Additional Details

- **Questions or Comments:**

  _____

  _____

  _____

Preference Checklist

- ☐ **Immediate Response Required**
- ☐ **Schedule a Service Demo**

Office Use Only

- **Handled By:** _____
- **Response Sent:** _____
- **Customer Feedback:** _____

3. Access Request Form

Data Subject Access Request Form

Please complete this form if you wish to request access to your personal data. You do not have to use this form, but it will help us to deal with your request as quickly and effectively as possible if you do.

You can also use this form if you are requesting access to personal data on behalf of someone else. In that case, we will need you to confirm you have that person's authority to ask for access to their data.

If you have any questions about this form or your request, please contact the Corporation's Data Privacy Officers to discuss it further.

1 About you

Please provide the following information. If you have an account number or other reference number, please provide it.

Full name	
Address	
Contact Email Address	
Contact Telephone	
Our Reference	

For security reasons, we cannot respond to a request unless we have confirmed your identity. Please provide:

- *a certified copy photo driving licence or passport, and*
- *a utility bill or other proof of address* that was dated no more than 3 months ago.

2 Whose personal data are you requesting?

Please provide the following information. If you are making this request on behalf of someone else, we will need this information before we can supply you with the data you are asking for.

Are you requesting access to your own personal data?	☐ Yes, please go to section 3 below. ☐ No, please complete the rest of this section of the form.

2.1 If you are not requesting access to your own personal data, please provide the following information about the person on whose behalf you are making this request:

Full name	
Address	
Contact details	
Our Reference	
Age (if under 16)	

We cannot respond to your request until we also receive satisfactory confirmation of the identity of the person on whose behalf you are making this request. Please provide:

- *a certified copy photo driving licence or passport, and*
- *a utility bill or other proof of address* which was dated no more than 3 months' ago.

2.2 Please provide a copy of your legal authority to make this request. This might be a signed letter of authority from the person on whose behalf you are making this request, a power of attorney, or confirmation that you are their legal representative.

3 What data are you requesting?

Your rights to request access to personal data and other information are set out in our Privacy policy, available on our website. Please describe what personal data and other information you are requesting, in particular, if you are asking for specific documents or information.

Description of the personal data and information requested including details of any specific documents or information you are asking for (where relevant)	

Please give as much detail as possible about where the data might be located and any other relevant information. You do not have to provide this information, but doing so will help us to deal with your request as quickly and effectively as possible.

Location of data, e.g. any particular departments or parts of the organization you have dealt with (if known)	
Relevant periods, e.g. when we are likely to have obtained your data (if known)	
Dates of any particular correspondence, meetings, or telephone calls (if known)	
The name(s) of people you have dealt with within our organization (if known)	
Any other relevant information you can think of that might help us respond to your request, including the types of matters we have assisted you with	

4 Signature

Please check the information you have provided and sign below.

Signed	
Date	

Please send this form and the documents we have asked you to provide at dataprotection@abcfinance.ph or call our dedicated privacy hotline at 09171071642.

If you are making this request by email, we will provide the information to you in an electronic format unless you ask us not to. If you wish to receive your information in a different format, e.g. hard copy please let us know in the box below.

4. Privacy Notice

DATA PRIVACY STATEMENT

ABC FINANCE CORPORATION (doing business under the name and style of 1 2 3 Finance Group) is committed to safeguard the personal and account information of our LOAN clients. In this regard, please be apprised of the regulatory requirements on data privacy and security.

Republic Act No. 10173 known as the Data Privacy Act (DPA) of 2012, issued by the National Privacy Commission (NPC) in August 2012, provides the guidelines on the implementation of this law. Please be informed that ABC FINANCE CORPORATION shall continue to process the personal, sensitive, and privileged information (collectively known as Personal Data) of its LOAN clients (who are regarded as the Data Subjects), in the course of its servicing of the clients' account/s with ABC FINANCE CORPORATION in accordance with applicable laws and regulations.

This Privacy Statement hereafter referred to as "Statement", explains how we collect, protect, use, and share your information when you access our websites and/or avail of our products and services.

This Statement outlines the general practices of ABC FINANCE CORPORATION in relation to our processes and content which are made available through our website and social media page. This Statement also covers the privacy practices for our customers who apply for and obtain loan products that ABC FINANCE CORPORATION may offer from time to time.

It is, however, the policy of ABC FINANCE CORPORATION to respect and uphold data privacy rights, and to ensure that all personal data collected from clients and employees are processed pursuant to the general principles of transparency, legitimate purpose, and proportionality as stated in DPA.

OUR PRIVACY PRACTICES

The privacy practices described in this Statement are primarily intended for individuals in the Philippines and are designed to comply with the Data Privacy Act of 2012 (R.A. 10173)and its implementing rules and regulations. When accessing our website and/or availing of our services from outside the Philippines, you acknowledge and agree that your information may be transferred to and processed in the Philippines following legal and regulatory standards for data protection that may differ from your current or home jurisdictions.

It is the policy of ABC FINANCE CORPORATION to respect and uphold data privacy rights, and to ensure that all personal data collected from clients and employees are processed pursuant to the general principles of transparency, legitimate purpose, and proportionality as stated in the Data Privacy Act of 2012.

The following information are necessary for our LOAN clients to know and understand:

Types of Information

- Personal information – any information, whether recorded in a material form or not, that will directly ascertain the identity of an individual. This includes your address and contact information.
- Sensitive personal information - personal information that includes:
    - About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political affiliations;

- About an individual's health, education, the genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
- Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
- Specifically established by an executive order or an act of Congress to be kept classified.

Privileged Information - any and all forms of information which, under the Rules of Court and other pertinent laws, constitute privileged communication, such as, but not limited to, information which a person authorized to practice medicine, surgery or obstetrics may have acquired in attending to a patient in a professional capacity.

Information We Will Collect From You

When you apply for or avail of any product or service, we collect your personal information so that we may provide valuable and useful services that we believe you might find interesting and beneficial. Personal information is any data that can be used to identify a person. This may include, among others:

- Your name and personal particulars such as contact details, address, birth date, education;
- Specimen signatures;
- Government ID details;
- Your name and personal particulars such as contact details, address, birth date, education; investments, tax, insurance, financial and transaction history, income, etc);
- Employment details;
- Business interests and assets;
- Images via CCTV and other similar recording devices and processes which may be observed when visiting our offices and/or using our other facilities;
- Voice recordings of our conversations with you

We may, as and when necessary, seek to verify or augment this information with third-party entities, including government regulators, judicial, supervisory bodies, tax authorities, orcourts of competent jurisdiction, and, in the process, gain additional information about you.

In the course of availing our products and services, we also collect information about your transactions and dealings which include your account activities, movements, andinteractions with third parties such as merchants and utility companies.

When you access our website, we may provide information about us as well as information regarding our products and services.

We may also collect, use and keep your personal opinions or comments made known to us via feedback or responses to surveys or any other interaction that you had with ouremployees, authorized representatives, agents, and service providers.

How We Use Your Information

We use the information collected to deliver and provide the products and services that you are to avail:

- Process applications and transactions for loans;
- Respond to queries, requests, and complaints and to improve how we interact with you;
- Send you statements, billings, notices, and other such documents necessary for continued use of our products and services;
- Conduct studies and researches to develop new or improve our existing products and services;
- Perform profile analysis, modeling, and analytics to better understand needs, preferences, and market trends for the development of more suitable products and services;
- To reach out to you regarding products and services information, including offers, promotions, discounts, rewards; and to know your experience with us thru our varioustouchpoints such as branches, call center, telemarketing, email, messaging, and other channels;
- Determine the effectiveness and sufficiency of our marketing efforts and initiatives;
- Provide location-based services such as finding the nearest branch to you, as well as reaching out our other services to you;
- Perform certain protective safeguards against improper use or abuse of our products and services including fraud prevention;
- Comply with our operational, audit, administrative, credit and risk management processes, policies and procedures, the terms and conditions governing our products,services, facilities and channels, the Securities and Exchange Commission rules and regulations, legal and regulatory requirements of government regulators, judicial,supervisory bodies, tax authorities or courts of competent jurisdiction, as to the same may be amended or supplemental from time to time
- To comply with applicable laws of the Philippines and those of other jurisdictions including the laws on the prevention of money laundering including the provisions ofRepublic Act No. 9160 (AntiMoney Laundering Act of 2001, as amended (AMLA) and the implementation of know your customer and sanction screening checks;
- Comply with legal and regulatory requirements such as submission of data to credit bureaus, credit information companies, the Credit Information Corporation (CIC)(pursuant to RA No. 9510 and its implementing rules and regulations) responding to court orders and other instructions and requests from any local or foreign authoritiesincluding regulatory, governmental, tax and law enforcement authorities or other similar authorities;
- Perform other such activities permitted by law or with your consent.

How We May Share Your Information

We may share your personal information with our subsidiaries, affiliates, and third parties, under an obligation of confidentiality.

- We may share personal information with various units within ABC FINANCE CORPORATION to better understand the way you use our products and services. This will allow us to improve our services and offer you opportunities to obtain such other useful products and services that may deliver greater value to you.
- We may share your information with our subsidiaries and affiliates to likewise offer you additional products and services that we believe you might find interesting.
- We may share with third parties that we engaged to support us in delivering our services to you.

- These may involve anonymous or aggregated information to help improve our products, services, and content.
    - We may also engage third parties to help us operate our business. These include support in:
    - Complying with legal requirements such as court orders;
    - Enforcing our terms of use including, among others, our rights as a creditor to customers availing of our loan products, or such other applicable policies with respect to the services that we provide;
    - Addressing fraud, security or technical issues, to respond to an emergency or otherwise to protect the rights, property, or security of our customers or third parties;
    - To carry out all other purposes set out above.

All our engagements with third parties shall be fully compliant with our obligation of confidentiality imposed on us under the applicable agreements and/or terms and conditions or anyapplicable laws that govern our relationship with you.

How We Protect Your Information

We fully recognize the value of your personal information particularly as it may include sensitive personal information such as your age, government-issued IDs, etc. Appropriately, we strive to maintain the confidentiality, integrity, and availability of your personal information by employing physical, technological, and organizational safeguards. We train our employees to properly handle your information. Whenever we engage other companies to provide services to us, we require them to protect personal information aligned with our security standards.

How Long Do We Keep Your Information

Your personal information shall be retained for as long as the purpose for which it was collected, and such other purposes that you may have consented to from time to time remains in effect until it is no longer required nor necessary to keep your information for any other legal, regulatory or business purposes.

OUR ROLE

We commit to use your personal information in the course of our financing relationship with you.

We shall use your information to determine what products and services we can provide you. Use of your information shall also be to comply with the legal and regulatory requirements of authorities such as the Securities and Exchange Commission (SEC), Credit Information Corporation (CIC), and our obligation to third parties. Non-identifiable data collected from our website visitors shall only be for tracking and servicing the users' concerns if any. We may also collect, process, store, and exchange your personal data in accordance with applicable laws and/or as per your agreement with us.

We ensure that your information with us is kept confidential.

We shall safe keep and use your information confidential within the bounds of applicable Philippine laws (e.g. Data Privacy Act of 2012; Credit Information System Act (R.A. No.9510); Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act; etc.). We shall provide only the needed information to government agencies, like the Bureau of Internal Revenue (BIR), and third parties when allowed by law and/or per your agreement with us.

We commit that the management of your personal information adheres to established security standards and procedures.

Our improved technology and information security framework shall prevent unauthorized access to your information which undergoes continuous assessment to improve securing your privacy.

YOUR RIGHTS

As provided under the DPA, you have the following rights in connection with the processing of your personal data: the right to be informed, right to object, right to access, right to rectification, right to erasure or blocking, and right to damages.

In respecting your privacy rights, you may opt to tell us:

1. Not to send you marketing materials via email;

2. Not to share your information with our subsidiaries and affiliates or with other companies that we have business with provided that such information is not critical nor required by applicable laws and regulations in maintaining the services that you have availed with us;

3. To provide you with information that we currently have about you subject to restrictions applied to us as a company operating in the Philippines by certain laws and regulations;

4. To update your information;

5. About your other concerns relating to how we collect, use, share, protect, or dispose of your information.

We may charge a fee for processing your request/s for access and/or update. Such a fee depends on the nature and complexity of your request. Information on the processing fee will be made available to you before making the request.

YOUR ROLE

Protect your personal information.

We entice you to be extra cautious in protecting your personal data by ensuring that your name, address, Identification Card Details (ID), and other important contact information arenot disclosed to other people, nor written where it will be easily accessible to others.

Report any data breach.

If you think that your personal data was improperly handled in terms of confidentiality or integrity, or if someone tampered with your personal data without your consent, pleasecontact us immediately thru our Data Protection Office, with contact details below:

Use secure means to contact us.

For any queries, clarifications, or requests on any aspect of this Statement, the exercise of your rights pertaining to your personal information, or to provide any feedback that you may have about our processing of personal information, please visit any of our branches or send us an email at dataprotection@abcfinance.ph or call our dedicated privacy hotline at 09171071642.

You may also write our Data Protection Officer at:

Data Processing Officer

ABC FINANCE CORPORATION

1600 Pedro Gil cor. J Bocobo St., Malate, Manila (across Robinson's Place Main Entrance)

CHANGES TO OUR PRIVACY STATEMENT

We may modify or amend this or amend this Privacy Statement from time to time to keep up with any changes in relevant laws and regulations applicable to us or how we collect, use, protect, store, share or dispose of your personal information. Any relevant updates will be posted on the Company's website.

5. Request for Correction or Erasure

REQUEST FOR CORRECTION AND ERASURE FORM

The Data Privacy Act of 2012 provides you ("the Data Subject" or "the Authorized Requestor", if not the Data Subject) with the **right to correct or remove the personal data** we, ABC FINANCE CORPORATION (collectively, the "Company") hold about the Data Subject. This form is used to confirm your identity and to assist us in locating your personal data.

This form can also be used to confirm the identity and authority of someone requesting on behalf of the Data Subject.

Your request will be processed within thirty (30) days of receipt of this form. We may require reasonably sufficient personal data from you to satisfy the Company as to your identity and to locate the personal data sought.

I. Data Subject Details

Full Name:			
Address:			
Email Address:		**Contact number (Telephone/Mobile):**	
Relationship to the Company:			

II. Authorized Requestor Details

Are you the Data Subject?	☐ Yes	☐ No

If you are **not** the Data Subject, you must supply the following documentary evidence to confirm the Data Subject's authority supporting this request:

☐ Duly notarized Special Power of Attorney from the Data Subject; or

☐ Appointment as receiver or administrator issued by a competent court.

If **authorized**, please provide the following information:

Full Name:			
Address:			
Email Address:		**Contact number (Telephone/Mobile):**	
Relationship to the Data Subject:			

I. Confirming Data Subject's Identity and Authorized Requestor's Identity

A. You must confirm the identity of the Data Subject by submitting us an **original or certified true copy** of one of the documents listed below. Please tick the appropriate box to indicate which document you have enclosed.

☐ Government-issued ID (TIN, NBI Clearance, Senior Citizen's ID, PRC ID, Driver's License, etc)
☐ Passport

If the Data Subject's name is different from the document or ID presented, you must supply a **copy** of documentary evidence to confirm the Data Subject's change of name (e.g., marriage certificate, change of name deed, or statutory declaration).

B. If you are **not** the Data Subject, you must confirm the identity of the Authorized Requestor by submitting us an **original or certified true copy** of one of the documents listed below. Please tick the appropriate box to indicate which document you have enclosed.

☐ Government-issued ID (TIN, NBI Clearance, Senior Citizen's ID, PRC ID, Driver's License, and so on)
☐ Passport

If the Authorized Requestor's name is different from the document or ID presented, you must supply a **copy** of documentary evidence to confirm the Authorized Requestor's change of name (e.g., marriage certificate, change of name deed or statutory declaration).

III. Confirming Authorized Requestor's or Data Subject's Mailing Address

If you opt to have your personal data mailed to the Authorized Requestor's or Data Subject's address, you must confirm your address by sending us a **certified true copy** of one (1) of the documents listed below. Please tick the appropriate box to indicate which document you have enclosed.

☐ Gas, electricity, water, or telephone bill in the Authorized Requestor's/Data Subject's name for the last quarter
☐ Income Tax Return in the Authorized Requestor's/Data Subject's name for the current financial year
☐ Bank or credit card statement in the Authorized Requestor's/Data Subject's name for the last quarter

IV. Correcting / Erasing the Personal Data of Data Subject

Details of the information you believe to be inaccurate and rectification required OR reason why you wish to have the personal data erased:

You must attach relevant documents as proof of correct information e.g., where a date of birth is incorrect, please provide us with a copy of the official Philippine Statistic Authority Birth Certificate. Please note that your right to request rectification/deletion is not absolute and may be declined by the Company in certain cases. You have the right to complain this refusal to the Office of the National Privacy Commission at complaints@privacy.gov.ph.

V. Methods of Notification

- ☐ I would like the reply to be delivered to the mailing address noted in the item III above.
- ☐ I would like the reply to be delivered through soft copy/scanned copy to my e-mail address.
- ☐ I would like to receive it personally by hand.

VI. Formal Declaration

In the exercise of the right granted to me under the terms of the Data Protection Act of 2012, I request that you correct or remove the personal data about the Data Subject which you process for the purposes I have indicated overleaf.

I confirm this is all of the personal data to which I am requesting access. I also confirm that I am either the Data Subject, or an authorized to act on their behalf. I am aware that it is an offence to unlawfully obtain such personal data, e.g., by impersonating the Data Subject or its authorized representative.

I certify that the information given in this form is true and accurate. I understand that it is necessary for the Company to confirm my/the Data Subject's identity and it may be necessary to obtain more detailed information in order to confirm my identity and/or locate the correct information.

By signing this form, I likewise explicitly and unambiguously consent to the collection, processing, and storage of the personal data provided in this Form for the purpose(s) of providing the access request which I hereby make and that which is stated in the Company's Data Privacy Manual (accessible *https://123finance.ph/)*

Signed by:

_____ _____

Signature over Printed Name Date (YYYY-MM-DD)