NATIONAL HOME MORTGAGE FINANCE CORPORATION

TERMS OF REFERENCE

HIRING OF DATA PRIVACY ACT (DPA) CONSULTANT

I. BACKGROUND

The National Home Mortgage Finance Corporation (NHMFC or the Corporation) was created by virtue of Presidential Decree No. 1267 dated December 21, 1977. The Corporation was classified as a Government Business Enterprise (GBE) under Commission on Audit (COA) Circular No. 2015-03 dated April 16, 2015.

In 2012, the Data Privacy Act 2012 which is a comprehensive and strict privacy legislation "to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth" (Republic Act No. 10173, Ch. 1, Sec. 2), was passed. Under the law, the National Privacy Commission (NPC) was created to serve as the enforcer and overseer of the Act. On September 09, 2016, the final implementing rules and regulations (IRR) came into force, thus mandating all covered entities both in the government and private sectors to comply.

In preparation for the assessment to be conducted by NPC, the Corporation would like to procure the services of a Data Privacy Consultant ("Consultant"), to assist the Corporation in complying with the provisions of the DPA, its IRR, and the relevant issuances of the NPC.

II. OBJECTIVE

The principal objective of this project is to ensure compliance with the applicable laws and regulations set for data protection (i.e., Five Pillars and 32-point Agenda of NPC) under the Data Privacy Act of 2021 which is being implemented by the National Privacy Commission (NPC).

III. SCOPE OF WORK

The consultancy agreement covers the engagement/hiring of a consultant through Competitive Bidding or Public Bidding, as provided under the 2016 Revised IRR of R.A. No. 9184. This project covers corporate wide processes and operations including the five (5) Regional and two (2) Satellite offices of NHMFC. The consultant to be hired shall perform the following:

Phase 1

1. Understand the current state of the Corporation;

1.1 Review the functions of the Data Protection Officer (DPO) and the required credentials, in accordance with/guided by NPC Advisory No. 17-01 which provides guidelines on the proper designation of a DPO, including the functions he or she is expected to perform, and provide recommendations.

1.2 Formulate the **Data Privacy Office Charter** - The charter defines and communicates the structure, duties and responsibilities of the DPO to ensure compliance with the requirements of Data Privacy Act (DPA) of 2012, its IRR and the related issuances by the NPC and other applicable laws and regulations.

1.3 Establish a baseline calendar of **the Data Privacy Office** - Refers to activities to be performed by the DPO and his/her support team throughout the year in compliance with R.A. 10173.

1.4 Assessment of NHMFC's compliance with the Data Privacy Act (DPA) of 2012.

2. Review the Corporation's existing policies on Data Privacy, including but not limited to policies on physical facilities relating to data security, data and information processed and stored in information systems, and recommend policies and/or changes in formal policies (i.e., Circulars, Memoranda, Office Orders, etc.) if necessary or when there is no existing policy/ies, on the following:

2.1 Data Subject Requests (User Access, Data Erasure and Data Correction handling procedures)

2.2 Data Subject Complaints

2.3 Data Destruction

2.4 Data Retention

2.5 Data Breach Management

3. Establish and conduct a Privacy Impact Assessment (PIA)

3.1 Preliminary

a. Make an inventory of personal data and provide data flow narratives (data life cycle)

b. Identify the projects, processes, programs, or measures that act on the data

c. Perform threshold analysis

d. Identify the risks associated with the processing of the personal data

3.2 Mobilize

a. Determine the plan and scope of PIA
b. Identify the resources needed

3.3 Conduct the PIA

a. Consult stakeholders, analyze risks, create risk map
b. Determine the necessary controls
c. Present the risks related to data privacy to the NHMFC Executive Committee, Risk Management Department (RMD) and Data Protection Office (DPO)

Phase 2

3.4 Implement the PIA which is part of or included in the DPA Manual

a. Deploy risk management controls related to Data Privacy Management
b. Recommend policies and procedures on monitoring and evaluation of PIA on a regular basis

3.5 Submit the PIA results to the DPO for acceptance and approval and present the same to the NHMFC Executive Committee for information and/or further instructions

3.6 Perform other activities related to the implementation of the PIA.

4. Formulate and conduct Privacy Management Program (PMP)

4.1 Governance

The first building block in the creation of PMP is the development of an internal governance structure that fosters a culture of privacy by defining the roles and processes on the following:

a. Management
b. Data Protection Officer
c. Reporting Mechanisms

4.2 Program Controls

Program controls will be used to demonstrate how the program is compliant with privacy legislation. These provide the framework for achieving the goals of the program, such as:

a. Records of Processing Activities
b. Risk Assessment
c. Registration
d. Policies and procedures for every stage of the data life cycle to ensure compliance with law and accountability in personal data processing.
e. Defined data security procedures on organizational, physical and technical security measures to maintain confidentiality, integrity, and availability of personal data.
f. Capacity building. Provide training materials and conduct trainings for NHMFC employees to comply with R.A. 10173.
g. Breach Management. Recommend policies, procedures and safeguards to manage security incidents, including personal data breaches.
h. Notification. Recommend policies and procedures to comply with notification requirements of the DPA.
i. Third-Party Management. Recommend policies and procedures to ensure proper safeguards of personal data when personal data is being processed/transferred by/to a third party.
j. Communication. Recommend policies and procedures to communicate with internal and external stakeholders.

4.3 Continuity and Maintenance of Privacy Management Program

This component outlines the critical tasks involved in the maintenance of a privacy management program to ensure ongoing effectiveness, compliance and accountability by providing the following:

a. Oversight and review plan. The plan must include performance measures and include a schedule of when all policies and other program controls will be reviewed.

b. Assessment and revision of program controls.

4.4 Modify the Privacy Management Program (PMP) into a Privacy Manual

Phase 3

5. Establish Privacy and Data Protection (PDP) Measures

5.1 Security Measures for Protection of Personal Data

a. Data Privacy and Security
b. Organizational Security
c. Physical Security
d. Technical Security
e. Appropriate Level of Security

5.2 Security of Sensitive Personal Information in Government
a. Responsibility of Heads of Agencies
b. Requirements Relating to Access by Agency Personnel to Sensitive Personal Information
c. Implementation of Security Requirements
d. Applicability to Government Contractors

5.3 Assist in the initial implementation of privacy and data protection measures.

6. Formulate Breach Reporting Procedures and Personal data breach management plan

6.1 Recommend how to respond internal incident report; and
6.2 Draft a Security Incident Management Policy aligned with the requirements of NPC Circular 16-03 on Personal Data Breach Management

The services to be rendered by the Consultant may be done within the NHMFC office premises, on-line or virtual conferencing depending on the given assignment, and subject to the approval of the Data Privacy Officer (DPO) or any of the latter's duly authorized representative, who will administer the project and deliverables.

IV. DURATION OF THE CONTRACT

The duration of the contract for hiring of Data Privacy Act (DPA) Consultant is one (1) year and shall commence fifteen (15) calendar days upon receipt of the Notice to Proceed (NTP).

V. RELATIONSHIP OF PARTIES

1. NHMFC will create a project team or committee to support the NHMFC designated DPO, the project team will act as project owner and partner of the DPA consultant during the engagement of the project.
2. No employer-employee or principal-agent relationship is created between the DPA consultant and NHMFC.
3. The DPA consultant shall assist or represent the NHMFC as may be required by government regulatory agencies, in matters related to RA 10173 or the Data Privacy Act 2012.
4. Other than the fees due to the DPA consultant at the time of the pre-termination or termination of the agreement, the consultant shall hold the Corporation free and harmless from any and all liabilities arising from or by reason of the Consultancy Agreement.

VI. REPORTING REQUIREMENTS

The DPA consultant shall submit an accomplishment report of services rendered to the DPO or any of the latter's duly authorized representative on or before the 25th day of every fourth month (trimester). The report to be submitted shall be in the form of e-file and hardcopies and shall be approved by the DPO or any of the latter's duly authorized representative. A printout bearing an attestation from the DPO or any of the latter's duly authorized representative that the same has been submitted within the deadline, shall be provided to the Consultant and kept on file by the Data Privacy Office.

Outputs/deliverables shall be submitted to the DPO or any of the latter's duly authorized representative and to the Executive Committee of the Corporation for acceptance and/or approval. The deliverables are as follows:

1. Schedule of Deliverables as stated in Scope of Work

PHASES	WORK OUTPUTS
Phase 1 Maximum of four (4) mos.	● Findings and Recommendations Report ● Data Protection Office Charter ● Calendar of Privacy Activities ● Assessment of NHMFC's Compliance with Data Privacy and Gap Analysis Report ● Data Protection Assessment Report ● Privacy Impact Assessment Report ● Conduct Privacy Impact Assessment
Phase 2 Maximum of four (4) mos.	● Privacy Management Program ● Data Privacy Manual includes PIA ● Privacy and Data Protection Measures
Phase 3 Maximum of four (4) mos.	● Regular status report of privacy activities ● Breach response test plan and result ● Data Breach Management Manual ● Incident Management Manual
	Certificate of Compliance with the Requirements of the Data Privacy Act of 2012 its IRR and other subsequent NPC issuances

2. Complete set of manuals, policies and guidelines on the said deliverables mentioned

3. Relative to the ongoing Pandemic due to COVID-19 virus being experienced by the entire country, the DPA consultant should provide a mechanism to adapt its team to the new normal and fully implement minimum health standards being required by the Corporation in conducting their activities within the NHMFC premises.

VII. TERMINATION

The contract may be terminated by the Corporation at any time even prior to the expiration of the period stated herein, in the event that the Corporation determines that it no longer needs the services of the DPA Consultant, or for any other reason, following the procedures and guidelines set forth in the procurement law (Republic Act No. 9184), its implementing rules and regulations, and pertinent jurisprudence on the matter.

VIII. CONFIDENTIALITY

The DPA Consultant will not, except as authorized or required by the DPA Consultant's duties herein stated, reveal or divulge to any person or entity any information concerning the organization, business, finances, transactions or other affairs of the Corporation which may come to the DPA Consultant's knowledge during the term of the Agreement and the DPA Consultant will keep in complete secrecy all confidential information entrusted to Consultant and will not use or attempt to use any such information in any manner which may injure or cause loss either directly or indirectly to the Corporation's interests.

IX. OWNERSHIP OF THE PROJECT

NHMFC shall have all the right, title and interest over all reports and data gathered by the Consultant and its team members/employees, together with the copyright, patent, trade secret and all other intellectual property rights of whatever nature gathered by the Consultant.

X. ADDITIONAL REQUIREMENTS

a. The Project Team Structure
b. Submission of financial statement for the last two (2) years

XI. APPROVED BUDGET OF THE CONTRACT

The Approved Budget of the Contract (ABC) is TWO MILLION **PESOS (2,000,000.00), inclusive of VAT and all applicable taxes and/or other miscellaneous expenses.**

XII. PAYMENT TERMS

The payment shall be based on the prescribed project timeline, to wit:

COMPLETION AND ACCEPTANCE	Percentage (%) of Contract Price
Phase 1 Deliverables	30%
Phase 2 Deliverables	30%
Phase 3 Deliverables Including the Certificate of Compliance with the Requirements of the Data Privacy Act of 2012 its IRR and other subsequent NPC issuances	40%
TOTAL	**100%**

XIII. PROJECT EVALUATION CRITERIA

Eligibility documents shall be evaluated using a non-discretionary "pass/fail" criterion as specified in the 2016 Revised Implementing Rules and Regulations (IRR) of Republic Act (RA) No. 9184, otherwise known as the "Government Procurement Reform Act".

The Consultant shall be evaluated based on the Technical and Financial proposal with a weight of 80% and 20% respectively. Overall passing rate of at least 80%.

THE TECHNICAL WORKING GROUP (TWG):

ANGELINA M. ANCHETA
Head

MA. NEMIA MARIENNE C. BENOSA
Member

NORA M. ENCINA
Member

EDMUNDO P. GARAIS
Member

MYRNA V. QUIMSON
Member

APPROVED BY:

NHMFC BIDS AND AWARDS COMMITTEE

Digitally signed by Cortez Carolina Cervania

CAROLINA C. CORTEZ
Member

Digitally signed by Favila Maria Luisa Merto

MARIA LUISA FAVILA
Member

Digitally Signed By

ATTY. DANTE M. PATAPAT
Member

Digitally signed by Roldan Romeo Salud

ROMEO S. ROLDAN
Vice-Chairperson

Digitally signed by Alpajaro Ma Victoria Listana

MA. VICTORIA L. ALPAJARO
Chairperson