

<b>MTC PRIVACY MANUAL</b>	Document No.	DPO-2025-002-01
	Effectivity Date:	20 MAR 2025
	Revision Date:	-
	Revision No.	Initial Issue
	Page No.	001-009
	Approval	Bill Ringer Salalima

21,  
[Redacted]  
[Redacted]



# MTC PRIVACY MANUAL

## 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.

It ensures that entities or organizations processing personal data establish policies, and implement measures and procedures that guarantee the safety and security of personal data under their control or custody, thereby upholding an individual's data privacy rights. A personal information controller or personal information processor is instructed 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 employees and personnel of Micropinnacle Technology Corporation ("MTC") of such measures, the company adopts this MTC Privacy Manual. The MTC Privacy Manual 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 National Privacy Commission (NPC). It also encapsulates the privacy and data protection protocols that need to be observed and carried out within MTC for specific circumstances (e.g., from collection to destruction), directed toward the fulfillment and realization of the rights of data subjects.

## II. Introduction

This MTC Privacy Manual is hereby adopted in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations, and other relevant policies, including issuances of the National Privacy Commission.

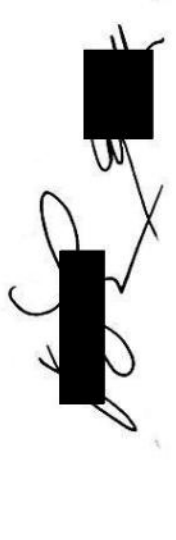
MTC respects and values your data privacy rights, and makes sure that all personal data collected from you, our clients and customers, are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality.

This MTC Privacy Manual shall inform you of our data protection and security measures, and may serve as your guide in exercising your rights under the DPA.

## III. Definitions

"Act" refers to Republic Act No. 10173, also known as the Data Privacy Act of 2012;

"Commission" refers to the National Privacy Commission;

Handwritten signature and redacted area.

"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 his or her personal, sensitive personal, or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so;

"Data subject" refers to an individual whose personal, sensitive personal, or privileged information is processed;

"Data processing systems" refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing;

"Personal data" refers to all types of personal information;

"Personal data breach" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed;

"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 natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:

1. A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
2. A natural person who processes personal data in connection with his or her personal, family, or household affairs;

There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing;

"Personal information processor" refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject;

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

manual processing, if the personal data are contained or are intended to be contained in a filing system;

"Security incident" is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of personal data. It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place;

"Sensitive personal information" refers to personal information:

1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
2. 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 individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
3. 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
4. Specifically established by an executive order or an act of Congress to be kept classified.

#### **IV. Scope**

All employees and personnel of MTC, regardless of the type of employment or contractual arrangement, including its service providers and contractors, must comply with the terms set out in this MTC Privacy Manual.

#### **V. Processing of Personal Data**

##### **A. Collection**

MTC collects the basic contact information of clients and customers, including their full name, address, email address, contact number. The assigned representative attending to the clients, for the purpose of providing business solutions and other services in accordance with the agreements (hereafter referred as "Services"), do not collect any data with regard to the clients of the customers.

##### **B. Use**

The personal data collected shall be used by MTC for documentation purposes, for communication and coordination in accordance with the employees and representatives of the customers of MTC in order to implement the Services.

### C. Storage, Retention, and Destruction

MTC ensures 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. The company will implement appropriate security measures in storing collected personal information, depending on the nature of the information. All information gathered shall not be retained for a period longer than three (3) years, unless required or requested by the data subject to be disposed or deleted. After three (3) years, all hard and soft copies of personal information shall be disposed and destroyed, through secured means.

### D. Access

Due to the sensitive and confidential nature of the personal data under the custody of the company, the authorized representative of the company shall be allowed to access such personal data, for any purpose, except for those contrary to law, public policy, public order or morals.

### E. Disclosure and Sharing

All employees and personnel of MTC 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 MTC shall be disclosed only pursuant to a lawful purpose, and to authorized recipients of such data.

## VI. Security Measures

### A. Organization Security Measures

MTC shall implement reasonable and appropriate physical, technical and organizational measures for the protection of personal data. Security measures aim to maintain the availability, integrity and confidentiality of personal data and protect them against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

The designated Data Protection Officer (DPO) is **Bill Ringer Salalima**.

The DPO ensures that the data protection rules are respected by:

1. Ensuring that controllers and data subjects are informed about their data protection rights, obligations and responsibilities and raise awareness about them;

2. Giving advice and recommendations to the management and stakeholders about the interpretation or application of the data protection rules;
3. Creating a register of processing operations for prior checks within the institution and notify MTC those that present specific risks;
4. Ensuring data protection compliance within MTC and aid to be accountable in this respect.
5. Handling queries or complaints on request by MTC, the controller, other person(s), customer or upon the DPO's initiative;
6. Cooperating with the customers of MTC and the Commission in responding to requests for investigations, complaint handling, inspections conducted by the Commission, etc.);
7. Drawing the management of MTC's attention to any failure to comply with the applicable data protection rules, if any;
8. Recommending and revisiting data privacy policies on a specified timeline or whenever needed.

MTC shall sponsor a mandatory training on data privacy and security at least once a year. For personnel directly involved in the processing of personal data, management shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.

MTC shall conduct a Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the processing of personal data. It may choose to outsource the conduct a PIA to a third party.

All employees, staff, personnel and service providers (hereafter referred as "employees") will be required to sign a Non-Disclosure Agreement. All employees with access to personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.

This Manual shall be reviewed and evaluated annually. Privacy and security policies and practices within MTC shall be updated to remain consistent with current data privacy best practices.

#### B. Physical Security Measures

MTC shall strictly follow the procedures intended to monitor and limit access to the facility containing the personal data, including the activities therein. It shall provide for the actual design of the facility, the physical arrangement of equipment and furniture, the permissible modes of transfer, and the schedule and means of retention and



disposal of data, among others. To ensure that mechanical destruction, tampering and alteration of personal data under the custody of MTC are protected from man-made disasters, power disturbances, external access, and other similar threats. Personal data in the custody of MTC may be in digital/electronic format and paper-based/physical format.

The physical security measures adopted by MTC are:

1. All personal data being processed by MTC shall be stored in a data room, where paper-based documents are kept in locked filing cabinets while the digital/electronic files are stored in computers provided and installed by the company.
2. Only authorized personnel shall be allowed inside the data room. For this purpose, they shall each be given a duplicate of the key to the room. Other personnel may be granted access to the room upon filing of an access request form with the Data Protection Officer and the latter's approval thereof.
3. All employees of MTC shall comply with the Clean Desk Policy such that every time a member is not in his/ her station, it is his/her responsibility to log out his/her computer device, keep drawers under lock and key, and secure all documents or devices containing personal data.
4. Employees authorized to enter and access the data room or facility must fill out and register with the online registration platform of MTC, and a logbook placed at the entrance of the room. They shall indicate the date, time, duration and purpose of each access.
5. The computers are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data. All portable devices capable of storage shall be prohibited in their workstations and shall be kept in store either at the employee locker or surrendered to a designated officer for safekeeping.
6. Persons involved in processing shall always maintain confidentiality and integrity of personal data. They are not allowed to bring their own gadgets or storage device of any form when entering the data storage room.
7. Transfers of personal data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments.
8. MTC shall retain the personal data of a client for three (3) years from the date of engagement, unless required or requested by the data subject to be disposed or deleted. Upon expiration of such period, all physical and electronic copies of the personal data shall be destroyed and disposed of using secure technology.

### **C. Technical Security Measures**

MTC implements technical security measures to make sure that there are appropriate and sufficient safeguards to secure the processing of personal data, particularly the computer network in place, including encryption and authentication processes that control and limit access. They include the following, among others:

1. MTC shall use an intrusion detection system to monitor security breaches and alert MTC of any attempt to interrupt or disturb the system
2. MTC shall first review and evaluate software applications before the installation thereof in computers and devices of MTC to ensure the compatibility of security features with overall operations.
3. Process for regularly testing, assessment and evaluation of effectiveness of security measures by reviewing security policies, conduct vulnerability assessments and perform penetration testing within the company on a regular schedule to be prescribed by the appropriate department or unit.
4. MTC uses encryption, authentication process, and other technical security measures that control and limit access to personal data by each personnel with access to personal data shall verify his or her identity using a secure encrypted link and multi-level authentication.

### **VII. Breach and Security Incidents**

A Data Breach Response Team comprising of five (5) officers shall be responsible for ensuring immediate action in the event of a security incident or personal data breach. The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. It shall also execute measures to mitigate the adverse effects of the incident or breach.

Bill Ringer Salalima	- Data Breach Response Head
Michelle Fulo	- Member
Atty. James Bryan O. Agustin	- Member
Gener P. Manantan	- Member
Joanne T. Lacap	- Member

MTC 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. Personnel directly involved in the processing of personal data are required to attend trainings and seminars for capacity building. MTC shall conduct a periodic review of policies and procedures being implemented in MTC.



MTC shall maintain a backup file for all personal data under its custody. In the event of a security incident or data breach, it shall always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the incident or breach.

The Head of the Data Breach Response Team shall inform the management of the need to notify the NPC and the data subjects affected by the incident or breach within the period prescribed by law. Management may decide to delegate the actual notification to the head of the Data Breach Response Team.

The Data Breach Response Team shall prepare a detailed documentation of every ticket, incident or breach encountered, as well as an annual report, to be submitted to management and the NPC, within the prescribed period.

### **VIII. Complaints / Requests**

Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of MTC, including the data privacy and security policies implemented to ensure the protection of their personal data. by filing a written complaint or request in three (3) printed copies or by sending an email to [dpo@mtc.com.ph](mailto:dpo@mtc.com.ph), briefly discuss the inquiry / request and contact details for reference.

### **IX. Effectivity**



The provisions of this MTC Privacy Manual are effective this 20 March 2025 until revoked or amended by this company, through a Board Resolution.



### **X. Annexes**

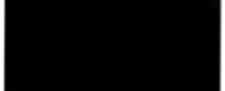

Attached to this MTC Privacy Manual are the following:

1. Data Privacy Consent
2. Data Privacy Inquiry Form
3. Access Request Form
4. Request for Correction or Erasure

In witness hereof, approved and signed by a Majority the Board of Directors of Micropinnacle Technology Corporation, on 20 March 2025, in Makati City, Metro Manila.

  
Gener Manantan  


  
Joanne Tan-Lacap  


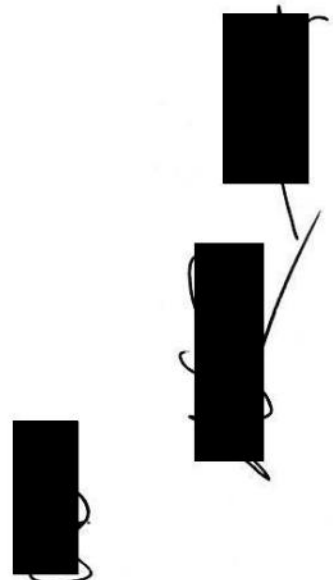
  
Michelle Fulo  


Prepared and recommended by:

  
**BILL RINGER SALALIMA**  
Data Privacy Officer

ANNEX 1

**DATA PRIVACY CONSENT**



### DATA PRIVACY CONSENT

By signing this consent form, I ("Data Subject") grant my free, voluntary and unconditional consent to the collection and processing of all Personal Data including records and documents submitted relating to me disclosed /transmitted by me in person or by my authorized representative to Micropinnacle Technology Corporation ("MTC"), in accordance with Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 and its Implementing Rules and Regulations.

I understand further, that, MTC, shall keep the personal data and information and the business and/or transaction that I do with MTC in strict confidence, and that the collection and processing of all personal data and/or information by MTC may be used for purposes of documentation and processing of my application, business transaction or negotiations for a possible business transaction.

At the same time, I agree that the information shall be shared to service providers, if necessary to achieve purposes mentioned and retained by MTC for as long as necessary for the fulfillment of the aforementioned purposes. I hereby acknowledge that I have been informed and provided notification on my rights as a Data Subject in accordance with the Data Privacy Act.

---

I have read and understood the above and hereby consent to, agree on, accept and acknowledge these terms of consent for myself by signing below.

Signed this \_\_\_\_ day of \_\_\_\_\_ 20\_\_ at \_\_\_\_\_ .

\_\_\_\_\_  
SIGNATURE OVER PRINTED NAME

[Redacted signature area]

[Redacted signature area]

ANNEX 2

**DATA PRIVACY INQUIRY FORM**





**DATA PRIVACY INQUIRY 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 access and receive a copy of the personal data. We, Micropinnacle Technology Corporation, ("MTC" or the "Company"), will use this form 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 making the request on behalf of the Data Subject.

Your request will be processed within thirty (30) days upon 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 requested before we can comply with your access request.

**I. Data Subject Details**

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

**II. Authorized Requestor Details**

<b>Are you the Data Subject?</b>	<input type="checkbox"/> Yes	<input type="checkbox"/> 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:

<b>Full Name:</b>			
<b>Address:</b>			
<b>Email Address:</b>		<b>Contact number (Telephone/Mobile):</b>	

<b>Relationship to the Data Subject:</b>	
--	--

**III. 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).

**IV. 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, telephone, utility bill in the Authorized Requestor's/Data Subject's name within the last quarter  
☐ Any Bureau of Internal Revenue 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  
☐ Any government issued ID bearing the address of the Authorized Requestor's/Data Subject's name

**V. Nature of Inquiry**

(Please check the applicable box)

- ☐ General inquiry about MTC's data privacy policies and practices
- ☐ Request for details on how my personal data is collected and processed
- ☐ Inquiry about my rights under the Data Privacy Act
- ☐ Inquiry about third parties who may have received my personal data
- ☐ Others (please specify): \_\_\_\_\_

Please provide a **detailed description** of your inquiry:

**VI. Preferred manner of compliance**

I would like to receive it in the form of \_\_\_\_\_ (e.g., USB, CD, printed copy, etc.)

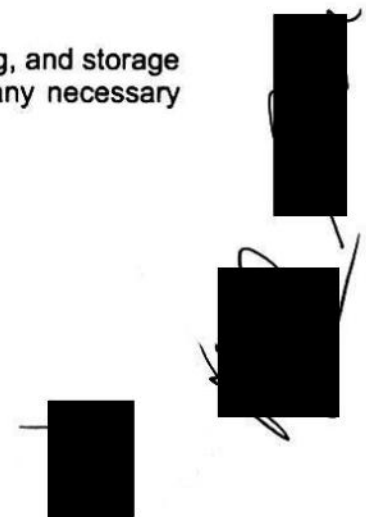
- ☐ I would like the reply to be delivered to the mailing address noted in the item IV above.
- ☐ I would like the reply to be delivered through soft copy/scanned copy to my e-mail address.
- ☐ I would like to receive it personally by hand.

**VII. Declaration and consent**

In line with my inquiry, I acknowledge that I am voluntarily providing my personal data to Micropinnacle Technology Corporation (MTC). I understand that my information will be collected, processed, and stored in accordance with the Data Privacy Act of 2012 and the Company's Privacy Policy, accessible at <https://www.mtc.com.ph/privacy-policy/>.

I certify that the information provided in this form is true and accurate. I understand that MTC may verify my identity and request additional details if necessary to process my inquiry.

By signing this form, I explicitly consent to the collection, processing, and storage of my personal data for the purpose of responding to my inquiry and any necessary follow-ups.



Signed by:

Signature over Printed Name	Date DD-MMM-YYYY
-----------------------------	------------------

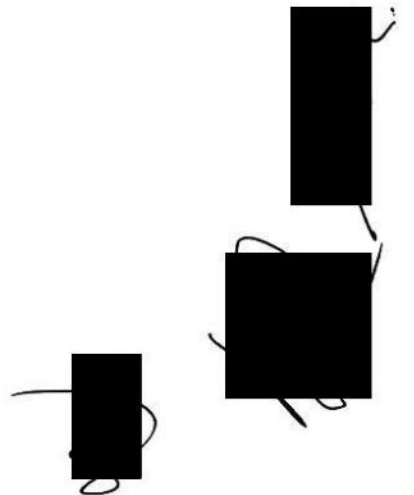
**Checklist.** Have you:

1. Completed the Inquiry Form in full? ☐
2. Enclosed the relevant form of identity and authority (see section 2) ☐
3. Enclosed the relevant form of identity and address (see section 3 and 4) ☐
4. Included document/s as proof of correct information? ☐
5. Signed and dated the Inquiry Form? ☐

Send the completed form and enclosures to:

**BILL RINGER SALALIMA***Data Protection Officer***MICROPINNACLE TECHNOLOGY CORPORATION**

Suite 7023 7th Floor, Golden Rock Building,  
168 Salcedo Street, Legaspi Village, Makati City  
[dpo@mtc.com.ph](mailto:dpo@mtc.com.ph)



ANNEX 3

**ACCESS REQUEST FORM**

[Redacted]  
[Redacted]  
[Redacted]



**ACCESS REQUEST 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 access and receive a copy of the personal data. We, Micropinnacle Technology Corporation, ("MTC" or the "Company"), will use this form 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 making the request on behalf of the Data Subject.

Your request will be processed within thirty (30) days upon 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 requested before we can comply with your access request.

**I. Data Subject Details**

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

**II. Authorized Requestor Details**

<b>Are you the Data Subject?</b>	<input type="checkbox"/> Yes	<input type="checkbox"/> 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:

<b>Full Name:</b>			
<b>Address:</b>			
<b>Email Address:</b>		<b>Contact number (Telephone/Mobile):</b>	

<b>Relationship to the Data Subject:</b>	
--	--

**III. 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).

**IV. 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, telephone, utility bill in the Authorized Requestor's/Data Subject's name within the last quarter  
☐ Any Bureau of Internal Revenue 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  
☐ Any government issued ID bearing the address of the Authorized Requestor's/Data Subject's name

**V. Requested Personal Data**

Our search for information relating to the Data Subject will be based on the information provided below. The Company processes personal data for the following purposes. Please tick the box(es) next to the purpose(s) that you would like us to search.

- ☐ Accounts and records
- ☐ HR and employment records
- ☐ Contracts
- ☐ <list other data that you are collecting>

**Description of personal information:**

*Please specify clearly and in detail the personal data requested (e.g., personal data contained in medical records, credit reports, employment evaluation, and vendor accreditation records). General description of the requested data, such as "all of my personal data", may render the request being refused by the Company as it may unreasonably locate the personal data to which the request relates to.*

**Any other information which will assist in searching for the personal data of the Data Subject?** (e.g., case or reference number and the name of the person in the Company you have had dealings with in the past, date of collection, and so on)


**VI. Preferred manner of compliance**

I would like to receive it in the form of \_\_\_\_\_ (e.g., USB, CD, printed copy, etc.)

- ☐ I would like the reply to be delivered to the mailing address noted in the item IV 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.

**VII. Declaration and consent**

In the exercise of the right granted to me under the terms of the Data Privacy Act of 2012, I request that you provide me with a copy of 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 am 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 Privacy Policy accessible at <https://www.mtc.com.ph/privacy-policy/>.

Signed by:

Signature over Printed Name	Date DD-MMM-YYYY
-----------------------------	------------------

**Checklist. Have you:**

1. Completed the Access Request Form in full?
2. Enclosed the relevant form of identity and authority (see section 2)
3. Enclosed the relevant form of identity and address (see section 3 and 4)
4. Included document/s as proof of correct information?
5. Signed and dated the Access Request Form?

- ☐
- ☐
- ☐
- ☐
- ☐

Send the completed form and enclosures to:

**BILL RINGER SALALIMA**

*Data Protection Officer*

**MICROPINNACLE TECHNOLOGY CORPORATION**

Suite 7023 7th Floor, Golden Rock Building,

168 Salcedo Street, Legaspi Village, Makati City

[dpo@mtc.com.ph](mailto:dpo@mtc.com.ph)



**ANNEX 4**

**REQUEST CORRECTION, AMENDMENT OR**

**ERASURE FORM**



**REQUEST CORRECTION, AMENDMENT OR 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 access and receive a copy of the personal data. Micropinnacle Technology Corporation ("MTC" or the "Company") will use this to confirm your identity and to assist us in locating, amending, correcting or erasing the personal data requested. This form can also be used to confirm the identity and authority of someone making the request on behalf of the Data Subject.

Your request will be processed within thirty (30) days upon 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 requested before we can comply with your access request.

**I. Data Subject Details**

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

**II. Authorized Requestor Details**

<b>Are you the Data Subject?</b>	<input type="checkbox"/> Yes	<input type="checkbox"/> 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:

<b>Full Name:</b>			
<b>Address:</b>			
<b>Email Address:</b>		<b>Contact number (Telephone/Mobile):</b>	

<b>Relationship to the Data Subject:</b>	
--	--

**III. 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).

**IV. 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, telephone, utility bill in the Authorized Requestor's/Data Subject's name within the last quarter  
☐ Any Bureau of Internal Revenue 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  
☐ Any government issued ID bearing the address of the Authorized Requestor's/Data Subject's name

**V. Inquiry of Personal Data**

Our search for information relating to the Data Subject will be based on the information provided below. The Company processes personal data for the following purposes. Please tick the box(es) next to the purpose(s) that you would like us to search.

- ☐ Accounts and records
- ☐ HR and employment records
- ☐ Contracts
- ☐ <list other data that you are collecting>

**Description of personal information:**

*Please specify clearly and in detail the personal data requested (e.g., personal data contained in medical records, credit reports, employment evaluation, and vendor accreditation records). General description of the requested data, such as "all of my personal data", may render the request being refused by the Company as it may unreasonably locate the personal data to which the request relates to.*

**Any other information which will assist in searching for the personal data of the Data Subject?** (e.g., case or reference number and the name of the person in the Company you have had dealings with in the past, date of collection, and so on)



**VI. CORRECTION, AMENDMENT OR ERASURE**

Please tick the box that is appropriate for the basis of your inquiry involving personal information:

☐ **CORRECTION**

PERSONAL DATA TO BE CORRECTED e.g. "John Doe"	CORRECTION
	"Jane Doe"

☐ **AMENDMENT**

PERSONAL DATA TO BE CORRECTED e.g. Date of Birth "01 January 2000"	CORRECTION
	"01 February 2000"

☐ **DATA TO BE DELETED**


USE ADDITIONAL SHEET PAGES IF NEEDED

**VII. Preferred manner of compliance**

I would like to receive it in the form of \_\_\_\_\_ (e.g., USB, CD, printed copy, etc.)

- ☐ I would like the reply to be delivered to the mailing address noted in the item IV 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.

#### VIII. Declaration and consent

In the exercise of the right granted to me under the terms of the Data Privacy Act of 2012, I request that you provide me with a copy of 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 am 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 Privacy Policy accessible at <https://www.mtc.com.ph/>.

By signing this form I understand that:

1. If the information requested reveals details directly or indirectly about another person, the Company will redact that information, or may seek the consent of that person before we can let you see that information.
2. In certain circumstances, MTC may deny the request, or may not be able to disclose information, in which case, a notice will be given promptly and given reasons for that decision.
3. While in most cases the Company will be happy to provide copies of the information requested, the Company nevertheless reserve the right to charge a fee or refuse the request, to the extent permitted under applicable law. However, the Company will make every effort to provide the requestor with a satisfactory form of access or summary of information if suitable.
4. The information provided will be used for processing Data Subject requests. The provision of personal data is voluntary. However, if the requestor does not provide sufficient information, the Company cannot process the request.

5. If the request is made by an individual other than the Data Subject, an authorization letter signed by the Data Subject and information that can provide proof of the identity of the Data Subject and further proof of the Requestor's status as a relevant person should be enclosed.
6. I may be asked to provide additional information to help the Company process my request, and I am required to provide proof of identity.

Signed by:

Signature over Printed Name	Date DD-MMM-YYYY
-----------------------------	------------------

**Checklist.** Have you:

1. Completed the Correction, Amendment, Erasure Form in full? ☐
2. Enclosed the relevant form of identity and authority (see section 2) ☐
3. Enclosed the relevant form of identity and address (see section 3 and 4) ☐
4. Included document/s as proof of correct information? ☐
5. Signed and dated the Correction, Amendment, Erasure Form? ☐

Send the completed form and enclosures to:

**BILL RINGER SALALIMA**

*Data Protection Officer*

**MICROPINNACLE TECHNOLOGY CORPORATION**

Suite 7023 7th Floor, Golden Rock Building,  
168 Salcedo Street, Legaspi Village, Makati City  
[dpo@mtc.com.ph](mailto:dpo@mtc.com.ph)