



# **PRIVACY POLICY OF M.B.A. CONSULTING PHILIPPINES INC.**

## **1. PRIVACY MANUAL**

## **2. DATA RETENTION AND DELETION**

## **3. CERTIFICATE OF NATIONAL PRIVACY COMMISSION OF THE PHILIPPINES ABOUT THE COMPLIANCE OF M.B.A. CONSULTING PHILIPPINES INC. WITH THE PERSONAL DATA PROTECTION POLICY IN ACCORDANCE WITH THE COUNTRY LEGISLATION**



# 1. M.B.A. CONSULTING PHILIPPINES PRIVACY MANUAL

## TABLE OF CONTENTS

### **Introduction**

### **Definition of Terms**

### **Scope and Limitations**

### **Processing of Personal Data**

- A) Collection
- B) Use
- C) Storage, Retention and Destruction
- D) Access
- E) Disclosure and Sharing

### **Security Measures**

- A) Organization Security Measures
- B) Physical Security Measures
- C) Technical Security Measures

### **Breach and Security Incidents**

- A) Creation of a Data Breach Response Team
- B) Measures to Prevent and Minimize Occurrence of Breach and Security Incidents
- C) Procedure for Recovery and Restoration of Personal Data
- D) Notification Protocol
- E) Documentation and Reporting Procedure of Security Incidents or a Personal Data Breach

### **Rights, Inquiries, and Complaints of Data Subjects**

### **Effective Date**



## INTRODUCTION

The purpose of the manual is to inform M.B.A. Consulting Philippines's clients and their contacts regarding how M.B.A. Consulting Philippines protects information, and to memorialize these efforts. M.B.A. Consulting Philippines adopts this Privacy Manual in compliance with Philippine Republic Act No. 10173 entitled "An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes" also known as the Data Privacy Act of 2012 ("DPA"), found at <https://www.privacy.gov.ph/data-privacy-act/> and its Implementing Rules and Regulations ("IRR") found at <https://www.privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012/>.

The DPA and IRR are intended to:

- (1) Protect the privacy of individuals while ensuring free flow of information to promote innovation and growth;
- (2) Regulate the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of personal data; and
- (3) Ensure that the Philippines complies with international standards set for data protection through Philippines National Privacy Commission ("NPC").

The DPA declares: "It is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected."

M.B.A. Consulting Philippines has reviewed its procedures, processes, protections, and practices as part of this commitment. M.B.A. Consulting Philippines is committed to privacy and to protect data that it processes. In particular, M.B.A. Consulting Philippines automatically secures the data of contacts that each of our clients uploads onto our site, so that only the client has usable access to that information. M.B.A. Consulting Philippines also has in place and is constantly and vigilantly upgrading its security defenses.

M.B.A. Consulting Philippines and its officers and employees respect and value individuals' data privacy rights and strive to make sure that any personal data on our site or that may otherwise come into our possession is dealt with and processed in adherence to the principles of transparency, legitimate purpose, and proportionality.

M.B.A. Consulting Philippines's Terms of Service (<https://ph.mbacgroup.com/terms>) and Privacy Policy (<https://ph.mbacgroup.com/privacy>) inform you about the information that may be uploaded onto M.B.A. Consulting Philippines, information we may gather, how we may use that information, whether we disclose it to anyone, and the choices you have regarding our use of the information we



process. We may update the Terms of Service, Privacy Policy and Privacy Manual as needed. This Manual will inform you of our data protection and security measures and may serve as your guide in exercising your rights under the DPA. If you have any questions or concerns, please, contact M.B.A. Consulting Philippines's Data Protection Officer at [dataprotectionofficer@ph.mbacgroup.com](mailto:dataprotectionofficer@ph.mbacgroup.com).

## DEFINITION OF TERMS

For the purposes of this manual, these terms are defined as follows:

**"Client"** or "M.B.A. Consulting Philippines client" is the entity or individual that uses M.B.A. Consulting Philippines's tools and expertise to communicate with others by means of SMS and telephone.

**"Client data"** is any and all information that the client provides to M.B.A. Consulting Philippines in order to become a client such as payment information as well as information relating to that client that M.B.A. Consulting Philippines may receive and use in order to better provide services to that client.

**"Contact"** is an individual or entity about whom the M.B.A. Consulting Philippines client uploads information onto M.B.A. Consulting Philippines. The client uses the various M.B.A. Consulting Philippines tools to organize the contacts to communicate with them via SMS and telephone.

**"Contact data"** is any data or information about contacts that the client uploads onto M.B.A. Consulting Philippines.

**"User"** is an individual who accesses the M.B.A. Consulting Philippines system with a user identification (e.g. email address) and password, API key, or other secure credential, and who may have access to client data and contact data for one or more clients.

**"User account data"** is client data that is associated with a particular user of the M.B.A. Consulting Philippines system.

**"Controller"** or "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 his/her behalf. A person or organization that performs such functions as instructed by another person or organization is not a controller. Generally, the M.B.A. Consulting Philippines client is the controller of the data the client uploads onto the M.B.A. Consulting Philippines site.

**"Personal Data"** refers to all types of personal information.

**"Personal Data Breach"** is 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.

**"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.



**“Processor” or “Personal Information Processor”** is any person, entity, or any other body to whom a “personal information controller” may outsource or instruct the processing of personal data pertaining to a data subject. Generally, M.B.A. Consulting Philippines is the processor of data as instructed by the M.B.A. Consulting Philippines client.

## **SCOPE AND LIMITATIONS**

All personnel of M.B.A. Consulting Philippines, regardless of the type of employment or contractual arrangement, must comply with the terms set out in this Privacy Manual and M.B.A. Consulting Philippines’s Terms of Service and Privacy Policy.

## **PROCESSING OF PERSONAL DATA**

M.B.A. Consulting Philippines treats all data, and particularly personal data, with the greatest of care and security.

When a M.B.A. Consulting Philippines client uploads any data or information regarding contacts (individuals or otherwise), that data is automatically and immediately secured. Contact data can be accessed only by users who were granted permission to access the contact data and who authenticate to M.B.A. Consulting Philippines with a password, API key, or other secure credential. In addition, M.B.A. Consulting Philippines maintains powerful security defenses that protect that data and information. These defenses are constantly monitored and assiduously upgraded.

**A) Collection of personal data:** M.B.A. Consulting Philippines client uploads onto the M.B.A. Consulting Philippines platform whatever information regarding individuals or otherwise that the M.B.A. Consulting Philippines client believes will assist it in pursuing its goals insofar as contacting by mobile message and/or by telephone members, customers, employees, organizations, or others. The M.B.A. Consulting Philippines client’s goals can be political, governmental, entrepreneurial, commercial, sales, personal, scientific, or otherwise. The uploaded information may include contacts’ names, addresses, email addresses, telephone numbers, political or other affiliations, age, marital status, and other personal or corporate information.

The client who uploaded this information has secure, password-protected access to it, and exclusively designates which users have access to this information in the M.B.A. Consulting Philippines system. M.B.A. Consulting Philippines personnel do not generally have access to this information nor know the identity of these contacts. The client utilizes M.B.A. Consulting Philippines’s tools in order to organize its contact data in a way to more efficiently and strategically communicate with its contacts.

In addition, if you are a client of M.B.A. Consulting Philippines, you provide certain information in order to access, use and pay for the M.B.A. Consulting Philippines tools as you see fit.





M.B.A. Consulting Philippines is generally used by for-profit and non-profit entities, clubs, organizations, businesses, and corporations. Each client typically has one or more users who are individuals and therefore upload user account data deemed to be personal data protected by the DPA and IRR.

M.B.A. Consulting Philippines may collect certain additional information on its clients in order to better serve that client, individual or otherwise, as explained more fully in M.B.A. Consulting Philippines's Terms of Service and Privacy Policy, including information about users' utilization and navigation of our Service such as the URLs a client visits before and after M.B.A. Consulting Philippines, Internet Protocol (IP) address, analytics data, log file information, and information collected with cookies. The collection of that data is part of the contract for services between the client and M.B.A. Consulting Philippines, and without collecting this data M.B.A. Consulting Philippines's processes would be less efficient. This data is stored in a secure manner that is only accessible by designated M.B.A. Consulting Philippines staff authenticated with secure credentials.

**B) Use:** As explained above, there are generally two categories of personal data on M.B.A. Consulting Philippines's site: data regarding clients ("Client Data") and data regarding clients' contacts ("Contact Data").

Client Data is comprised of the data uploaded onto M.B.A. Consulting Philippines's site by a client in order to allow it access to the M.B.A. Consulting Philippines services and tools, and includes communication and payment information, as well as data for each user account associated with that client, such as their name and email address.

Use of client data focuses on improvement of services to the client and will be used in the same way as more fully set forth in M.B.A. Consulting Philippines's Terms of Service and Privacy Policy.

Contact Data is any data or information about contacts that the client uploads onto M.B.A. Consulting Philippines. Use of Contact Data is controlled entirely by the Client.

**C) Storage, Retention and Destruction:** Client and contact data is stored and processed by means of servers situated in the Philippines only. M.B.A. Consulting Philippines ensures that all data, including personal data, under its custody is protected against any accidental or unlawful destruction, alteration, or disclosure as well as against any other unlawful processing. The same security and other protection processes are used wherever client and contact data is stored and/or retained. M.B.A. Consulting Philippines considers protection of client and contact data to be one of its most important and critical services and is constantly vigilant regarding security. M.B.A. Consulting Philippines has no hard copies of any electronic data relating to clients or contacts.

Following the deletion of contact data from the M.B.A. Consulting Philippines service, M.B.A. Consulting Philippines may retain the deleted contact data for a commercially reasonable time for backup, archival, or audit purposes. In no case shall this time be greater than six (6) months following deletion of contact data.



Following termination of a M.B.A. Consulting Philippines user account or client account, M.B.A. Consulting Philippines may retain the associated user account data or client data for a commercially reasonable time for backup, archival, or audit purposes. In no case shall this time be greater than six (6) months following termination of the user account or client account.

**D) Access:** Regarding all contact data uploaded onto M.B.A. Consulting Philippines by clients that may include personal data, all that data is secured so that only that client and individuals the client designates have access to it. Only the client has usable access to its contact data.

It is extremely important that users keep their password and other credentials completely confidential. If you are a user of M.B.A. Consulting Philippines, anyone with access to your user identification and password will be able to view the confidential information that you are authorized to access and communicate with Contacts as if that person were you. If you have a user account with an associated API key, anyone with access to that API key would be also able to access the M.B.A. Consulting Philippines REST API if that person were you. Additionally, anyone with access to your email account could reset your password on the Service to access your account on the Service as if that person were you.

To reduce the risk of user accounts being compromised, M.B.A. Consulting Philippines allows clients to configure additional security restrictions for their account. Clients that want to prohibit access to their contact data from outside their corporate network may configure a whitelist of IP addresses that are allowed to access their M.B.A. Consulting Philippines account. In addition, M.B.A. Consulting Philippines supports two-factor authentication using one-time passwords. M.B.A. Consulting Philippines provides the ability for clients to require their users to enable two-factor authentication before accessing contact data.

To become a client of M.B.A. Consulting Philippines, certain limited information regarding name and payment details must be provided. Only the client and authorized employees of M.B.A. Consulting Philippines have access to this information. As more fully explained in M.B.A. Consulting Philippines's Privacy Policy, M.B.A. Consulting Philippines also collects certain technical information regarding the client in order to better serve and protect that client, including: information about users' utilization and navigation of our Service such as URLs a client visits before and after M.B.A. Consulting Philippines, Internet Protocol (IP) address, analytics data, log file information, and information collected with cookies. The collection of that data is part of the contract for services between the client and M.B.A. Consulting Philippines, and without collecting this data M.B.A. Consulting Philippines's processes would be less efficient. All of this information is securely stored and access to the information is controlled via secure credentials. Only M.B.A. Consulting Philippines's Chief Technology Officer and technical staff under NDA have access to this technical information.

**E) Disclosure and Sharing:** All M.B.A. Consulting Philippines employees and personnel maintain the confidentiality for all data and information regarding clients that come to their knowledge and



possession, even after resignation, termination of contract, or other contractual relations. Personal data under the custody of M.B.A. Consulting Philippines shall be disclosed only as permitted by applicable law and pursuant to a lawful purpose as set forth in the Terms of Service and the Privacy Policy, and to contractual relations.

## **SECURITY MEASURES**

M.B.A. Consulting Philippines considers security regarding the information that is uploaded onto or otherwise on its platform by M.B.A. Consulting Philippines Clients to be of the utmost and critical importance. As a personal information controller or personal information processor, an organization must 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 client and contact data and protect that data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination.

### **A) Organization Security Measures**

- 1.** All employees and contractors have signed, and new employees and contractors will sign a Confidentiality Agreement. All employees with access to personal data operate and hold personal data under strict confidentiality.
- 2.** M.B.A. Consulting Philippines has appointed a Data Protection Officer (“DPO”) who can be contacted at [dataprotectionofficer@ph.mbacgroup.com](mailto:dataprotectionofficer@ph.mbacgroup.com). M.B.A. Consulting Philippines’s DPO has direct access to M.B.A. Consulting Philippines’s Chief Executive Officer and Chief Technology Officer and has the authority to contact any and all employees and contractors of M.B.A. Consulting Philippines.
- 3.** The Data Protection Officer oversees M.B.A. Consulting Philippines’s operations insofar as compliance with all laws and regulation worldwide regarding the protection of personal information, including the DPA and IRR. The Data Protection Officer has direct access to any and all officers and personnel of M.B.A. Consulting Philippines in order to ensure compliance. The Data Protection Officer will be apprised of any and all security issues, incidents, breaches, complaints or inquiries, and will deal with them accordingly. The Data Protection Officer will be apprised of any upgrades or changes to M.B.A. Consulting Philippines’s security system and measures and have input regarding these. The Data Protection Officer will be a resource for all employees in pursuit of protecting the privacy rights of all individuals.
- 4.** The DPO shall provide updates, trainings and/or seminars to keep personnel apprised vis-à-vis developments in data privacy and security.
- 5.** All personnel shall be required to read and review the Terms of Service, Privacy Policy, and





this Privacy Manual within one month of the publication of this Manual or within one month he/she first becomes employed. All personnel shall be informed of any changes to these documents that affect the protection and confidentiality of personal data insofar as M.B.A. Consulting Philippines's operations.

**6.** The DPO shall be the first contact for any client, contact or anyone else with questions, complaints, or concerns regarding the protection of privacy rights. The DPO's email address shall be conspicuously placed on the pertinent online documents and pages to ensure that clients, contacts, contractors, personnel, visitors, and government officials can communicate with the DPO easily and quickly.

**7.** M.B.A. Consulting Philippines implemented security policies for managing security and security incidents prior to the DPA and IRR. M.B.A. Consulting Philippines considers security one of its most critical tasks. M.B.A. Consulting Philippines constantly reviews its security policies.

**8.** The DPO shall record, and document activities carried out by the DPO and M.B.A. Consulting Philippines to ensure compliance with the DPA, its IRR and other relevant policies.

**9.** Review of Privacy Manual. This Manual shall be reviewed and evaluated annually. Privacy and security policies and practices within the organization shall be updated to remain consistent with current data privacy laws, regulations, and best practices.

## **B) Physical Security Measures**

The data relating to clients and their contacts is stored and processed on servers situated in the Philippines only. These servers can be provided by third-party private entities, including Google and Amazon, that protect and maintain them under the highest standards. M.B.A. Consulting Philippines considers security to be one of the key aspects of its service to its clients and their contacts.

**1.** All personal data is kept in digital/electronic form and is on securely hosted servers in locations in the Philippines only with state-of-the-art security.

**2.** Only the Chief Technology Officer and designated technical staff have login access to servers with access to client data or contact data.

**3.** The servers are kept in extremely secure facilities that are under constant surveillance with access limited only to technical personnel who ensure the servers are operating properly.

**4.** Remote login access to the servers from the internet is blocked by a firewall and is only available by technical staff connecting via a secure VPN with multi-factor authentication.

## **C) Technical Security Measures**

M.B.A. Consulting Philippines has in place the following technical security measures:

**1.** Monitoring for security breaches: Each of M.B.A. Consulting Philippines's servers are monitored by intrusion detection software which alerts M.B.A. Consulting Philippines



technical staff for potential security breaches.

**2.** Security features of the software and applications used: M.B.A. Consulting Philippines's software is designed to avoid web application vulnerabilities including, but not limited to, cross-site scripting (XSS), cross-site request forgery (CSRF), and SQL injection. M.B.A. Consulting Philippines constantly reviews and improves its software security.

**3.** Process for regularly testing assessment and evaluation of effectiveness of security measures: M.B.A. Consulting Philippines uses vulnerability monitoring systems to automatically notify technical staff of vulnerabilities in third-party software components used on M.B.A. Consulting Philippines's servers. M.B.A. Consulting Philippines also maintains automated tests which validate security-related aspects of the M.B.A. Consulting Philippines software, including the user permissions system. Review of M.B.A. Consulting Philippines's security is an ongoing endeavor led by the Chief Technology Officer, assessing any potential vulnerabilities.

**4.** Password protection, authentication process, and other technical security measures that control and limit access to personal data: All contact data and client data is secure and accessible through the M.B.A. Consulting Philippines service only via user accounts authenticated with password, API key, or other secure credentials. If someone attempts to log in with an invalid password multiple times for the same user account or from the same IP address in a short time interval, the user account will automatically be locked in a short period of time to prevent automated guessing of user passwords. Clients may also enable two-factor authentication via a time-based one-time password (TOTP) distributed by Google Authenticator, SMS, or voice call. Clients may also enable a whitelist of internet protocol (IP) addresses that are allowed to access their data. Access to data by M.B.A. Consulting Philippines employees and contractors is tightly controlled by the Chief Technology Officer.

## **BREACH AND SECURITY INCIDENTS**

**A)** Data Breach Response Team: Response to any data breach will be led by the Chief Technology Officer who will obtain the assistance of any employees or contractors necessary to assess, mitigate and prevent any further breach.

**B)** Measures to prevent and minimize occurrence of breach and security incidents:

M.B.A. Consulting Philippines constantly assesses security to avoid any risks or vulnerabilities in M.B.A. Consulting Philippines's system and network.

**C)** Procedure for recovery and restoration of personal data: M.B.A. Consulting Philippines maintains a backup file for all personal data under its custody. In the event of a security incident or data breach, it shall compare the backup with the affected file to determine the presence of any inconsistencies



or alterations resulting from the incident or breach.

**D)** Notification protocol: The Chief Technology Officer shall consult with the Chief Executive Officer and the Data Protection Officer of the need, if any, to notify the Philippine National Privacy Commission and the data subjects affected by the incident or breach within the periods prescribed by law, which may be as short as 72 hours.

**E)** Documentation and reporting procedure of security incidents or a personal data breach: The Chief Technology Officer shall work with the Chief Executive Officer, the Data Protection Officer, and others as needed in the preparation of documentation of every incident or breach encountered to be submitted to the NPC, within the prescribed period.

## **RIGHTS, INQUIRIES AND COMPLAINTS OF DATA SUBJECTS**

Under the laws of the Republic of the Philippines, every individual has:

- (a)** A right to reasonable access to her personal information.
- (b)** A right to rectification or correction of her personal information if it is incorrect.
- (c)** A right to object to the processing of her personal information by M.B.A. Consulting Philippines.
- (d)** A right to erasure or blocking of her personal information.
- (e)** A right to portability whereby M.B.A. Consulting Philippines will transfer her personal information to another entity of her choice.
- (f)** A right to lodge a complaint before the Philippine National Privacy Commission.

Inquiries or requests may be made regarding any matter relating to personal data and M.B.A. Consulting Philippines, including M.B.A. Consulting Philippines's data privacy and security policies. A form is attached to this Manual, which may be of assistance. Anyone may correspond with M.B.A. Consulting Philippines at [dataprotectionofficer@ph.mbacgroup.com](mailto:dataprotectionofficer@ph.mbacgroup.com) and relate the details of the issue, together with contact information for response.

Complaints should be sent to [dataprotectionofficer@ph.mbacgroup.com](mailto:dataprotectionofficer@ph.mbacgroup.com). Any complaint must provide the name and contact information of the complainant and explain the complaint and basis therefor. If third parties are involved, their names and contact information should be provided as well. The Data Protection Officer shall confirm with the complainant the receipt of the complaint, may contact the complainant seeking additional and/or more specific information, shall investigate the complaint as necessary and appropriate, and shall respond as appropriate to the complaint within a reasonable period.

## **EFFECTIVE DATE**

The provisions of this Manual are effective this 05th day of March 2022, until revoked or amended by the Chief Executive Officer or the Chief Technology Officer.



## 2. DATA RETENTION AND DELETION

### DATA RETENTION

In Chapter III, Section 11.e: General Data Privacy Principles of Data Privacy Act of 2012, Personal Information must be retained only for as long as necessary for the fulfillment of the purposes for which data was obtained.

The following are the purposes:

- a) Data are retained for the purpose of billing.
- b) For the establishment, exercise, or defense of legal claims, call recordings are retained for reviewing complaints.

All data will be retained for three (3) months for its purpose and call recordings are stored for six (6) months per M.B.A Consulting PH standard but not limited to the requirement presented by the client per Service Level Agreement (SLA).

### DATA DELETION

Files that are due for deletion will be deleted either Physically or Electronically. This will be mandatory to be able to save space on our servers.

Physical data will be deleted and purged using an in-house paper shredder in the presence of either the IT Manager or the Operations Manager.

Electronic data that are due for deletion will be deleted and purged only by an authorized person assigned. These data will be completely deleted from our system storage to save some space for new data. Will then create a certificate of deletion upon the request of the client including the name of the client who owns the data, number of cases deleted, date of deletion, and date of endorsement to be signed by the Operations Manager and IT Manager.



# DPO/DPS

DATA PROTECTION OFFICER

DATA PROCESSING SYSTEM

**REGISTERED**

**“DATOS NG PILIPINO,  
PROTEKTADO KO!”**



VALIDITY PERIOD:

23 May 2024

A handwritten signature in black ink, appearing to read "J. Naga", written over a horizontal line.

Atty. John Henry D. Naga  
PRIVACY COMMISSIONER