[POP-UP]

COOKIE NOTICE
We use cookies to ensure you receive the best experience from our website. By clicking "I AGREE" or continuing to use the website, you accept the use of cookies. Your data will be processed in accordance with our **Data Privacy Policy** and **Cookie Policy**.

COOKIES NOTICE

CAZA Technology Solutions Inc. ("CAZA") is committed to safeguarding your personal information, and we wish to be transparent about how we handle the same.

Accordingly, we developed this Cookie Notice to inform you about our use of cookies across this website. We want you to understand what cookies are, how CAZA uses cookies, and what your choices are.

A cookie is a small piece of data (text file) that a website - when visited by a user - asks your browser to store on your device in order to remember information about you, such as your language preference or login information. Those cookies are set and called first-party cookies. We also use third-party cookies - which are cookies from a domain different than the domain of the website you are visiting - for our advertising and marketing efforts. More specifically, we use cookies and other tracking technologies for the following purposes:

- **Strictly Necessary Cookies.** These cookies are necessary for the website to function and cannot be switched off in our systems. CAZA embeds cookies that are essential for navigating and enabling functionalities such as local device authentication, animation, and image caching. These cookies are turned on by default. If you set your browser to block these cookies, some parts of the site will not work.

- **Performance Cookies.** CAZA uses cookies to understand how visitors use the website and its services in order to improve the over-all performance. Performance cookies provide insights into trends and usage patterns that are used for business analysis, website and service improvements, and for determining performance metrics.

The use of cookies also depends on the settings of the web browser you are using (e.g., Microsoft Edge, Google Chrome, Apple Safari, Mozilla Firefox). Most web browsers are preset to automatically accept certain types of cookies. However, you can usually change this setting. You can delete stored cookies at any time. Web/DOM storage and local shared objects can be deleted separately. You can find out how this works in the browser or device you are using in the manual of the learner.

The consent to, and rejection or deletion of, cookies are tied to the device and also to the respective web browser you use. If you use multiple devices or web browsers, you can make decisions or settings differently.

If you choose to delete or refuse to accept cookies, you may not have access to some or all functions of our website or individual functions may be limited.

WEBSITE, COOKIES & SIMILAR TECHNOLOGIES TRACKING POLICY

When you visit our websites, cloud and online services, software products, or view our content on certain third-party websites, we collect information regarding your connection and your activity by using various online tracking technologies, such as cookies, web beacons, Local Storage, or HTML5. Information that is collected with these technologies may be necessary to operate the website or service, to improve performance, to help us understand how our online services are used, or to determine the interests of our users. We may use advertising partners to provide and assist in the use of such technologies on CAZA website and other sites.

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 CAZA of such measures, the company adopts this Privacy Manual. The 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 CAZA for specific circumstances (e.g., from collection to destruction), directed toward the fulfillment and realization of the rights of data subjects.

II. Introduction

This 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.

CAZA 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 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;

“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 CAZA, regardless of the type of employment or contractual arrangement, must comply with the terms set out in this Privacy Manual.

V. Processing of Personal Data

A. Collection

CAZA 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 data analytics 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 CAZA for documentation purposes, for communication and coordination in accordance with the employees and representatives of the customers of CAZA in order to implement the Services.

C. Storage, Retention, and Destruction

CAZA 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 one (1) year. After one (1) year, 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, only the client and 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 CAZA 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 CAZA shall be disclosed only pursuant to a lawful purpose, and to authorized recipients of such data.

VI. Security Measures

A. Organization Security Measures

CAZA 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.

CAZA designates a Data Protection Officer.

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 CAZA those that present specific risks;

4. Ensuring data protection compliance within CAZA and aid to be accountable in this respect.

5. Handling queries or complaints on request by CAZA, the controller, other person(s), customer or upon the DPO’s initiative;

6. Cooperating with the customers of CAZA and the Commission in responding to requests for investigations, complaint handling, inspections conducted by the Commission, etc.);

7. Drawing the management of CAZA'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.

CAZA 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.

CAZA 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 CAZA shall be updated to remain consistent with current data privacy best practices.

B. Physical Security Measures

CAZA 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 CAZA are protected from man-made disasters, power disturbances, external access, and other similar threats, the physical security measures adopted by CAZA are:

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

2. All personal data being processed by CAZA 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.

3. 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.

4. All employees of CAZA 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.

5. Employees authorized to enter and access the data room or facility must fill out and register with the online registration platform of CAZA, and a logbook placed at the entrance of the room. They shall indicate the date, time, duration and purpose of each access.

6. The computers are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data. All portable device capable of storage shall be prohibited in their workstations and shall be kept in store either at the employee locker or surrendered to a designate officer for safekeeping.

7. 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.

8. Transfers of personal data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments.

9. CAZA shall retain the personal data of a client for one (1) year from the data of purchase. 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

CAZA 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. CAZA shall use an intrusion detection system to monitor security breaches and alert CAZA of any attempt to interrupt or disturb the system.

2. CAZA shall first review and evaluate software applications before the installation thereof in computers and devices of CAZA 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 regular schedule to be prescribed by the appropriate department or unit.

4. CAZA 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.

CAZA 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. CAZA shall conduct a periodic review of policies and procedures being implemented in CAZA.

CAZA 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 CAZA, including the data privacy and security policies implemented to ensure the protection of their personal data. Briefly discuss the inquiry / request / complaint and provide contact details for reference.

Written inquiries / requests / complaints may be sent to:

Data Protection Officer
CAZA Technology Solutions Inc.
Unit 707 Antel Corporate Center
121 Valero Street, Salcedo Village,
Makati City

Or by sending an email to dataprivacy@cazatechnology.com.

IX. Effectivity

The provisions of this Privacy Manual are effective this 18th day of January 2024 until revoked or amended by this company.

X. Annexes

Attached to this Privacy Manual are the following:

1. Consent Form
2. Inquiry Form
3. Access Request Form
4. Request for Correction, Amendment or Erasure Form