DATA PRIVACY POLICY

Introduction

Overview

In line with the Company's purpose and values, Satellite Office (hereby referred to as "the Company") places great importance on your right to privacy and is compliant with Republic Act 10173, or the Data Privacy Act of 2012. We continuously ensure compliance with the provisions of the said acts and all of its aspects to protect the information you provide the Company, specifically in line with the following aspects:

- Data collection and processing
- Storage, security, and access
- Data correction and disposal
- Maintaining open lines for communication and reporting

Scope

The scope of the policy shall cover the manner, usage and protection of data collated by the Company both from internal and external data collection points. These shall include all but not limited to:

- Job applicant information
- Company employee information
- Company and personal information of vendors and providers
- Information gathered from website visitors

The policies and principles of Privacy Policy shall likewise apply to independent contractors, personnel working on our premises who are employed by temporary agencies and any other persons or firms doing business for or with the Company.

If the data subjects that we collect information from are not listed in this privacy policy, these individuals will be given appropriate notice of which data will be collected and its usage (when required by law).

Definition of Personal Information

For the purpose of this policy, the definition of "personal information" is defined in Republic Act 10173. "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.

Data Collection and Processing

Data is collected for varied purposes. All of which, alongside its processing methods are detailed in this section.

Categories, Types, and Purposes of Personal Information Collection

Job applicant information

Types of Information

- Full name, Place of Residence (current and permanent), Contact numbers (mobile and/or landline), Email address
- Work History (names of previous employers, previous job titles, employment dates, job coverage and responsibilities, projects and achievements), Educational Background (schools attended, course or degree completed, dates attended)
- Names of character references, names of character references' employers, contact number/s of references, relationship with references, availability of references for contact
- Age, Gender, Date of Birth, Place of Birth, Family background (number of siblings, children, etc.), Marital status
- Medical history, results of medical exams, Identification numbers of government benefits, criminal records

Purpose

- Basic information for contact and identifier of data ownership
- Ensuring candidate suitability for the role candidate is profiled for or applying for
- Conducting reference checks as part of the screening process
- Profiling for improvement of company benefits, engagement programs
- Compliance with government regulations for onboarding new employees

Company employee information

Types of Information

- Employment contract and agreements, attendance record, tax status, payroll record
- When using company-issued equipment: websites visited, application usage, file access, productivity movements and statistics, location of equipment, keystrokes, chat messages, email activity, email content, webmail content
- Corporate email address, corporate contact numbers
- Username and passwords of accounts in company and/or client systems (e.g. HRIS, ATS, systems used in fulfilling role responsibilities
- Medical history, medical records which may include results of medical exams, procedures, and consultations

- Identification numbers of government benefits, criminal records, information related to applications to avail of government benefits
- Biometric data, media captured by CCTV and other monitoring systems
- Media captured during events (photographs, video, audio)

Purpose

- Perform payroll and other administrative functions
- Monitor proper usage of company-issued equipment
- Dissemination of information and corporate communication
- Proper administration of administrative, support, system, and operational functions
- Documentation on fit-to-work assessments, regulations on health and wellness
- Proper administration of benefits
- Implementation of security measures
- Employment branding

Company and personal information of vendors and providers

Types of Information

- Full name (point of contact, account manager/s, etc.), Office address/es, Contact numbers (mobile and/or landline), Email address, hours of operation
- Industry, business model, schedule of operations, manpower headcount, offered solutions, pricing, strategic and other future business plans
- Name of authorized signatory, designation of authorized signatory, granted special arrangements

Purpose

- Basic information for contact and identifier of data ownership
- Assessment of offered and available solutions
- Creation and execution of Services Agreement

Information gathered from website visitors and potential clients

Types of Information

- Identifiers (IP address, handles on social media accounts, email address, phone number/s), browser / web data and browsing preferences
- Cookies and geolocation data
- Name, location data, contact details (email, phone numbers)

Purpose

- Creation of more relevant and suitable solutions
- More optimized browser experience
- Basic information for contact and identifier of data ownership

Information collected shall be processed for the purposes mentioned above based on your prior consent, to the extent that such consent is mandatory under applicable laws.

Once you select "I accept", "I agree" or similar offered options in relation to a privacy policy, doing so will be considered as providing us with your consent to process your personal information, only where such consent is required by mandatory law.

Personal information will not be processed or used for purposes that are not aligned with what has been communicated to you by authorized representatives of the Company, unless it is required or authorized by law, or it is in your own vital interest (e.g. in case of a medical emergency) to do so.

Sensitive Personal Information

"Sensitive personal information", as defined by relevant acts, refers to personal information specifically identified as requiring special treatment. These categories include racial or ethnic origin, political opinions, religious, philosophical or other similar beliefs, membership of a trade union, physical or mental health, biometric or genetic data, sexual life or orientation, or criminal convictions and offences (including information about suspected criminal activities).

The Company generally does not require the collection of sensitive personal information aside from the redefined purposes detailed in this policy. In the event that such data is needed and is either not listed in the table above and/or will be used for purposes not aligned with definitions detailed in this policy, we will explicitly communicate the need with you and collect the information in accordance with data privacy law requirements and/or ask for your consent.

Data Collection Sources

Personal information not provided voluntarily and directly from you may be obtained by the Company from the following sources:

- Publicly available digital sources, such as the internet or public social media profiles;
- Company employees, as with the case of employee referrals;
- Access of the Company website;
- Submission of inquiries, requests, applications and other transactions done through Company and affiliate channels, such as, but not limited to, online and offline events, campaigns, and drives;
- Use of electronic devices including personal computers, laptops, and other work equipment issued by the Company;
- Providers and partner companies, such as job boards, medical providers, and background check providers;
- Previous employers;
- Schools and educational institutions attended;
- Company's current clientele;
- Company affiliates, subsidiaries, stakeholders, and other personal contacts that you may or may not have had recent interaction with;
- Public authorities and documents that are publicly available.

Regardless of the jurisdiction covering the parties that the Company and its authorized representatives interact with, the Company ensures that the acts referred to in this policy,

alongside all similar acts in the jurisdiction not mentioned in this policy, are complied with to the full extent that the respective acts require.

Data for Marketing Purposes

Sources of Marketing Data

The bulk of personal information that the Company collects and uses for marketing its job vacancies and company events relates to job applicants, employees of our clients, internal support employees, and other individuals who we may have done business with and/or have subscribed to receive such communication. Contact information is also collected from visitors of our website, participants of marketing campaigns and events, and from public sources, including publicly-available content, social media websites, and similar sources. The purpose of this collection is to make initial contact with an interested individual/s.

Cookies and Tracking Technologies

The Company may also collect personal information through the use of cookies. A "cookie" is a piece of information that is collected to allows the server to identify and interact more effectively with the device used. This assists us in maintaining the continuity of your browsing session (i.e. to prevent repetitive processes to be undertaken by the browsing party) and in remembering details and preferences when you return. This also enables us to track services you view so that, if you consent, we can send you relevant information about these services. We also use cookies to measure web traffic activity and patterns to determine which functionalities and areas have been visited and to measure transaction patterns.

Other similar technologies that may be used in this regard include web beacons (which may operate alongside cookies) and JavaScript. Some of these cookies and other technologies are consistent across our digital platforms, providing us with information to understand your interests better and provide a better user experience across these platforms.

As with popular tracking technologies, the Company analyzes your IP address, location data (if available and not disabled), dates, times, file metadata, referring website/s, data entered, user activity such as links clicked and browser information to determine user experience and website features that works best for you. This is to help us identify ways to improve user interfaces, content, and functionalities, and, eventually, to determine how we can redesign our website for a more positive and relevant user experience.

You can use browser configurations and settings to disallow and delete cookies, as well as to block JavaScript. This may limit functionality of our website services.

Rights in Relation to Marketing Communication

The right to prevent marketing communications can be exercised by choosing the relevant options on the forms used to collect your personal information, or through opt-out mechanisms in emails sent to you. You can also exercise the right to discontinue the Company's marketing communications with you, or to have personal information removed from our CRM databases at any time by contacting the Company's Data Privacy Officer.

If opting out has been availed, the Company will retain minimum personal information to note that opting out was availed so as to avoid having members contact you in future campaigns.

Storage, Security, and Access of Personal Information

Disclosure and Sharing of Personal Information

As a company existing in Australia and the Philippines, personal information collected may be processed in either or both countries. The Company has stringent measures implemented that limit the access of such information only to the parties authorized by both the Company and relevant acts for the purposes declared in this policy.

The Company may disclose collected personal information to the following:

- Company employees, clients, service providers and/or partners and affiliates for operational and/or business purposes, and/or as part of fulfilling requests lodged by the party providing the personal information;
- Government institutions in the Company's compliance with statutory and legal mandates;
- Any other individuals, or entities for any authorized purposes with your express consent.

Personal information may also be shared to individuals/entities overseas, subject to the requirements and limitations under relevant acts and governing laws.

The Company may transfer personal data to partner and/or affiliate companies, clientele, providers, public and governmental authorities, or third parties in connection with the Company's operation of its business, with purposes of which including any existing or prospective corporate and/or commercial transaction. As these third parties may be located in other countries, the Company takes the necessary measures to ensure that personal information will be protected in alignment with relevant acts and data privacy laws.

The Company may also share your information for the purpose of substantial corporate

transactions, such as the sale of a website, a merger, consolidation, asset sale, initial public offering, acquisition, or in the unlikely event of a bankruptcy.

Data Security

The Company's IT resources are managed alongside a third-party provider. Together, we ensure the physical, technical, and organizational security arrangements for all collected and stored personal information. The Company and its leadership have designed and implemented controls as well as policies, procedures, protocols and guidance to maintain the utmost security, and continuously update the content of all measures so as to account for the risks associated with the categories of personal data and the processing undertaken by respective individuals and teams associated with the Company.

The security measures implemented by our third-party provider abides by international security standards and is designed to, first and foremost, protect the personal information stored within its systems. As an example, our third-party provider has successfully been awarded the ISO 27001 certification year on year. This means that all legal, physical and technical controls involved in an organization's information risk management processes have been audited and have been found to be fully compliant. Simply stated, the presence of the ISO 27001 certification means that the Company's systems adhere to the best in class methods and policies to secure its systems.

On top of this, our provider taps its resources and networks to perform regular penetration testing and ensure that the robustness of its cybersecurity measures.

As a Company, the systems used by internal support teams as well as implemented workflows undergo full and regular due diligence so as to ensure that data collection, storage, security, and disposal all adhere to global data protection standards.

Rights to Access of Personal Information

Although extensive efforts are undertaken by the Company to ensure that collected data is complete and kept up-to-date, the accuracy is ultimately dependent on the quality of the information that you provide us. This is where you may practice your rights to access your personal information, which are summed up as follows:

- Right to object to the processing of personal information – you may request for the Company to no longer process your personal information for direct marketing, automated processing or profiling. The limitations of such rights are aligned with the relevant Acts used as a basis in creating this policy.
- Right to access your own personal information that was collected for processing – you may request for information on whether we hold personal data about you and, if we do, obtain details on the stored personal information. You may also request for a copy of the aforementioned personal information stored in our system/s.

- Right to rectification of personal information – you may dispute the inaccuracy in the collected and stored personal information and have the Data Privacy Officer correct this immediately and accordingly. Such requests shall be reviewed and corresponding actions may or may not be taken depending on the reasonability of the request. Once corrected, you shall be provided with a copy of both new and retracted information, and all parties to whom the information was shared with shall be made aware of such correction.
- Right to erasure or blocking of your personal persona information – you may request for your personal data to erased and properly disposed from our system/s in alignment with the predefined conditions in the relevant Acts.
- Right to portability of your personal information – you may request for a copy of the personal information that you have provided to the Company, which shall be provided in a structured, commonly used and machine-readable format.

Contacting the Data Privacy Officer

Process of Raising Concerns and Complaints

To exercise any of the above listed rights, we encourage you to contact our Data Privacy Officer whose details are listed below.

Similarly, complaints regarding data privacy violation under the relevant Acts and this policy may be raised to the Data Privacy Officer through written complaint, either handwritten with the signature of the complainant affixed or electronically typewritten with a digital signature of the complainant affixed, attaching all substantial document providing such data privacy violation and personal data breach.

The Data Privacy Officer or authorized representatives will contact you within ten (10) business days to confirm receipt of your complaint. A response to the complaint/s shall be provided within a reasonable time frame.

Following the exhaustion of all available remedies, a complaint may be lodged under the Data Privacy Act of 2012 before the National Privacy Commission. Contact information is listed in the following section.

Nikko Tani

Director of Account Management
Satellite Office Solutions Pty Ltd – Philippine Branch
19th/20th Floor Uptown Place Tower 2, 11th Avenue corner 11th Drive
Bonifacio Global City, Taguig City 1634
Email Address: mailto:nikkot@satelliteoffice.com
Office Number (AU): +61 2 8317 2773
Mobile Number (PH): +63 (0)917 805 3515

National Privacy Commission
5th Floor, Delegation Building, PICC Complex
Roxas Boulevard, Pasay City, Metro Manila 1307
Landline: (+632) 2342228
Email Address: complaints@privacy.gov.ph
Website: https://www.privacy.gov.ph/