MPI Privacy Policy

Version 6

MicroSourcing

Contents

Revision History

Version	Date	Author	Approved By	Description
1	11 May 2017	John Joenelle Nudo	Sjoerd Krosse	Initial Release
2	9 August 2019	John Joenelle Nudo	Sjoerd Krosse	Revised DPO details/Additional References
3	6 October 2019	John Joenelle Nudo	Sjoerd Krosse	Revised DPO contact numbers/Revised address of NPC and added complaints web address
4	29 February 2020	Niño Christopher Pura	Sjoerd Krosse	Revised DPO contact details
5	5 March 2020	Niño Christopher Pura	Sjoerd Krosse	Changed name of parent company
6	1 July 2021	Carlo Valencia Bernadette Jean Frias	Jo Zarapoulos Niño Christopher Pura	Revised DPO details/Updated Guidelines

Document Information

I. Introduction

MicroSourcing Philippines, Inc. (“MicroSourcing” or “Company”) values the importance of protecting the privacy and the rights of individuals in relation to their personal information. This includes existing and prospective customers of our clients, potential and existing employees and contractors whom MicroSourcing collects personal information from or is provided with such information from our clients. The MicroSourcing Privacy Policy details how the company uses and protects all personal data in accordance with Republic Act 10173, otherwise known as, the Data Privacy Act of 2012 (“DPA”), its implementing Rules and Regulation (IRR), other issuances of National Privacy Commission (NPC), other relevant laws of the Philippines and also adopt generally accepted international principles and standards such as Australian Privacy Act 1988 (Cth) and the New Zealand Privacy Act 1993.

II. MicroSourcing Privacy Policy Statement

This Policy aims to further enforce and comply with all applicable and data protection laws for personal data and ensure that SPI (sensitive Personal Information) will consistently safeguard the fundamental human right of every individual to privacy.

Our commitment reflects the value we place on earning and keeping the trust of our customers, business partners and others who share their personal information with us. In this regard, we would like to inform you as to how your personal data will be used. Hence, we recommend that you read this Privacy Policy for you to better understand our data collection, use, processing, disclosure, storage and retention and policy. Your submission of data to us shall be treated as your consent and express permission for all necessary and applicable disclosures referred to in this Privacy Policy.

III. Personal Information and Sensitive Personal Information

1. When used in this Privacy Policy, the term “personal information” has the meaning as defined underthe relevant Act. This refers to any information, whether recorded in a material form or not, from whichthe identity of an individual is apparent or can be reasonably and directly ascertained by the entityholding the information, or when put together with other information would directly and certainlyidentify an individual.

2. Sensitive Personal Information (SPI) refers to Personal Data covering the following:

    - Individual’s race, ethnic origin, marital status, age, color, and religious, philosophical orpolitical affiliations;
    - individual’s health, education, genetic or sexual life, or to any proceeding for anyoffense committed or alleged to have been committed by such individual, the disposalof such proceedings, or the sentence of any court in such proceedings;
    - issued by government agencies peculiar to an Individual which includes, but is notlimited to, social security numbers, previous or current health records, licenses or itsdenials, suspension or revocation, and tax returns; and
    - specifically established by an executive order or an act of Congress to be kept classified.

IV. General Principles of Collection, Hold, Use & Disclosure of Personal Information

1. We collect personal information about you so that we can perform our business activities and functions and to provide the best possible quality of customer service to you and to enable us to provide products and services to our clients.

2. We collect, hold, use and disclose your personal information for the following purposes, in each case, either on our own behalf or when acting on behalf of a client:

    - To provide products and services to you and our clients and to send communications requested by you and/or our clients;
    - to answer inquiries and provide information or advice about existing and new products or services;
    - to conduct business processing functions including providing personal information to our related bodies corporate, clients, contractors, field officers, service providers or other third parties;
    - to assess the provision of, and provide credit, to you;
    - to undertake debt collection services on behalf of our clients;
    - for the administrative, marketing (including direct marketing), planning, product or service development, quality control and research purposes of MicroSourcing, its related bodies corporate, clients, contractors or service providers;
    - to provide your updated personal information to our related bodies corporate, clients, contractors or service providers;
    - to update our records and keep your contact details up to date;
    - to process and respond to any complaint made by you; and
    - to comply with any law, rule, regulation, lawful and binding determination, decision or direction of a regulator, or in cooperation with any governmental authority of any country (or political subdivision of a country).

3. Where you are our employee, we may collect, hold, use and disclose your personal information for all purposes connected with our employment relationship. This includes hiring you, training you, administering your personnel records (including pay and leave records), and managing your performance.

4. We may also use your personal information for other purposes related to those described above, and/or for a purpose for which you would reasonably expect it to be used, as permitted by the applicable Act.

5. MicroSourcing may also handle sensitive personal information pursuant to the exceptions provided under the Data Privacy Act of 2012.

6. All personal information collected will not be shared, sold, rented or disclosed other than as described in this Privacy Policy. We do not disclose personal

V. Data Processing of Personal Information

Adequate records of the Company's Personal Data Processing activities shall be maintained at all times. The Data Protection Officer ("DPO") and/or Compliance Officer for Privacy ("COP") with the assistance of the concerned Site Leads involved in the Processing of Personal Data, shall be responsible for ensuring that these records are kept up-to-date. These records shall include at the minimum:

- Information about the purpose of the Processing of Personal Data, including any intended future processing or data sharing;
- a description of all categories of Data Subjects, Personal data and recipients of such Personal Data that will be involved in the processing;
- general information about the data flow within the Company, from the time of collection and retention, including the time limits for disposal or erasure of Personal Data;
- a general description of the organizational, physical, and technical security measures in place within the Company; and
- the name and contact details of the DPO, Personal Data Processors, as well as any other staff members accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.

A. Personal information we collect and hold

1. We may collect the following types of personal information and sensitive personal information:

- Name;
- signature;
- mailing or street address;
- email address and telephone and facsimile number;
- age or birth date;
- system access passwords;
- profession, occupation or job title;
- where you are our employee, your personnel records including your employment agreement, pay records, leave records, tax status, criminal record checks, superannuation records, training records, and performance and disciplinary records;
- or our customers (on whose behalf we may provide products or services) or which you have inquired about, together with any additional information necessary to deliver those products and services and to respond to your inquiries;
- where you are a customer of our client and we are discussing overdue debts, details of your employment and bank account details;
- credit card details;
- details of your creditworthiness and credit history;
- any additional information relating to you that you provide to us directly or indirectly through our websites and/ or through our official social media accounts; and
- information you provide to us through our service center, customer surveys or visits by our representatives from time to time.

2. We may also collect some information that is not personal information because it does not identify you or anyone else. For example, we may collect anonymous data or aggregated information about how users use our websites. We do not re-identify this information to turn it into personal information.

B. How do we collect your personal information?

The DPO with the assistance of the Site Leads on all MicroSourcing offices/branches shall document the Company's Data Processing Procedures. It is the responsibility of the DPO/COP to ensure that such procedures are updated and that the consent of the Data subjects is properly obtained and evidenced by written, electronic, or recorded means. Such procedures shall also be regularly monitored, modified, and updated to ensure that the rights of the Data Subjects are respected, and that the Processing thereof is done fully in accordance with the Data Privacy Act and/or other applicable laws and regulations.

As a business process outsourcing and offshore leasing company, MicroSourcing is provided with personal information by our clients collected from individuals or entities from foreign jurisdictions. When collecting personal information, we may collect in ways including:

a. Use and access of MicroSourcing website/s;
b. use of telephone or mobile communication devices;
c. use of electronic devices including personal computers, laptops and tablets issued by the company;
d. conversations with our officers, employees, relatives, contractors, assigns and representatives;
e. in some cases, we may also collect your personal information through the use of cookies;
f. when completing an application, contract or purchase order;
g. through information collected and shared by our affiliates, subsidiaries, contractors and sub-contractors.

MicroSourcing, in the course of its operations, may also collect personal information from third parties who are not our clients, affiliate or subsidiary. This includes recruitment firms, background investigation firms and third-party providers.

MicroSourcing will not collect, disclose or process personal data, including data that may be classified as personal information and/or sensitive personal information unless you voluntarily give your consent thereto or unless such disclosure is required by applicable laws and regulations.

In our commitment to demonstrate transparency when processing your personal data, we will require you to read, understand and sign the Privacy Notice and Consent forms before we collect your personal information. In some cases, however, collection of information may only require verbal consent when deemed practical and/or necessary:

- **Privacy Notice**
  Information on collection and processing of personal data of the Data Subjects shall be relayed to the Data Subject through a Privacy Notice. The Company's Authorized Personnel shall inform the Data Subject of the purpose/s of the collection and processing of personal data, and the Rights of the Data Subject with regard to privacy and data protection.

- **Consent**
  The Consent of the Data Subject shall be evidenced by the Data Subject's signature or conformity which may be provided either in writing or by any electronic means (e.g. e-signature, etc.).

C. What happens if we can't collect your personal information?

If you do not provide us with the personal information described above, some or all of the following may happen:

a. We may not be able to provide the requested products or services to you, either to the same standard or at all, or we may not be able to supply services to our clients which will enable our clients to do the same; or
b. we may not be able to provide you with information about products and services that you may want, including information about discounts, sales or special promotions, or we may not be able to supply services to our clients which will enable our clients to do the same; or
c. we may not be able to tailor the content of our websites to your preferences, or we may not be able to supply services to our clients which will enable our clients to do the same; or
d. if you are a client of ours, we may not be able to provide you with the products and services you require; or
e. if you are a prospective employee, we may not be able to hire you; or
f. if you are our employee, it may be a breach of your employment conditions to not provide us with the required information; or
g. if you are a contractor to us, you may not be able to provide your services to us.

D. How MicroSourcing uses your personal information

MicroSourcing mainly collects personal information from the following:

a. Our valued clients; and
b. applicants and employees.

The Company's use of the Personal Data shall only be for the purpose of carrying out the business operations of the Company. The Processing of Personal Data of Data Subjects shall be for the following general purposes, among others to:

a. Document and manage Company records;
b. conduct due diligence prior to executing a contract, and to facilitate the fulfillment of the terms of the contract or master of services agreement (MSA) thereafter;
c. respond to queries, complaints, and requests;
d. provide information about Company services;
e. conduct research and analysis to improve customer experience and customer valued services;
f. maintain security;
g. comply with legal, regulatory, and contractual requirements or obligations.

The use and processing of Personal Data also depends on the Company transactions involved.

MicroSourcing only collects personal information which is reasonably necessary and/or directly related to the one or more of MicroSourcing's functions, business and activities.

E. To whom may we disclose/share your personal information?

1. MicroSourcing may disclose your personal information to the following:

    a. Our employees, clients, contractors or service providers for the purposes of operation of our websites or our businesses, fulfilling requests by you, and to otherwise providing products and services to you and our clients including, without limitation, web hosting providers, IT systems administrators, mailing houses, couriers, payment processors, data entry service providers, electronic network administrators, debt collectors, and professional advisors such as accountants, solicitors, business advisors and consultants;
    b. our subsidiaries, affiliates and related companies, and their directors, officers, and employees;
    c. suppliers, clients and other third parties with whom we have commercial relationships, for business, marketing, credit reporting and related purposes;
    d. government agencies in relation to MicroSourcing's compliance with its statutory and legal mandates;
    e. any other individuals, or entities for any authorized purposes with your express consent.

2. Personal information may be combined and/or shared with other information, personal or otherwise, collected by MicroSourcing or other individuals/entities. Our clients may do likewise.

3. **Overseas Disclosure**
    We may disclose personal information to our related bodies corporate and third-party suppliers and service providers located overseas for some of the purposes listed above. Some of our employees are located overseas. Except where specific individual consent has been obtained, we take reasonable steps to ensure that the overseas recipients of your personal information do not breach the privacy obligations relating to your personal information.

    Personal information may also be shared to individuals/entities overseas, subject to the requirements and limitations under the Acts.

F. How long do we keep and store your personal data?

- Personal data of the data subjects collected, used and disclosed by the Company shall only be retained:

    Personal Information shall be retained only for as long as necessary for the fulfillment of the purposes for which data was obtained. Such purpose/s may include but not limited to the following:

    1. For the fulfilment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated; or
    2. for the establishment, exercise or defense of legal claims; or
    3. for the legitimate business purposes, which must be consistent with standards followed by the Company or approved by appropriate government agency; or
    4. in any case provided by law.

- Personal Data shall only be stored for as long as necessary to carry out an aspect of the business operation of the Company. The purposes for which it was collected and processed, as well as the applicable periods prescribed by law, if any, shall be considered in retaining the Personal Data.

How long we retain Personal Data:

1. For financial data collected, Company Document or Records and Hard copy Materials- ten (10) years based on required retention period as mandated by the Philippine laws; or
2. for personnel records collected, two (2) years after termination; or
3. for CCTV recordings, retention of records in the system is for sixty (60) days, in cases where there is breach in security, the company shall store the recording of the footage for ten (10) years or for as long as necessary to fulfill the purposes for which the CCTV footage was obtained.

Where we store your Personal Data

The Personal Data of Data Subjects shall be stored in the pertinent Information and Communication Systems, such as but not limited to, password-protected computer devices, secure filing cabinets, secure filing rooms and other storage devices. Where necessary to further its business and to keep its security software tools up-to-date, the Company reserves the right to change and/or update its Information and Communications Systems and Filing Systems.

G. How do we dispose your personal data?

Upon expiration of the Retention Period, all physical and electronic copies of the Personal Data shall be destroyed and disposed of using secure means that would render the personal Data unreadable and irretrievable to prevent the occurrence of any Personal Data Breach and other Security Incidents.

All files that contain personal data must be securely disposed, destroyed or permanently de-identify, whether such files are:

1. Stored on paper, film, optical or magnetic media; and
2. any computer equipment, such as disk servers, desktop computers and mobile phones at end-of-life (especially storage media) provided that the procedure shall include the use of Physical destruction devices or degaussers (a machine that disrupts and eliminates magnetic fields stored on tapes and disk media, removing data from devices like your hard drives);
3. stored offsite, outsourced, or subcontracted.
4. Provided, that the Company has no legitimate reason for retaining such files.

VI. Cookies

This is a piece of information that allows the server to identify and interact more effectively with your device.

We provide information and services ourselves and on behalf of our clients through a range of digital and online services including websites, apps, email, online advertisements, and social media profiles ("Digital Services"). These services may be operated by us to provide a consistent experience, personalize your use of each of those services and to provide targeted marketing.

The cookie assists us in maintaining the continuity of your browsing session (e.g. to maintain a shopping cart) and remembering your details and preferences when you return. It also enables us to keep track of products or services you view so that, if you consent, can send you news about those products or services.

We also use cookies to measure traffic patterns, to determine which areas of our website have been visited and to measure transaction patterns in the aggregate. We use this to research our users' habits so that we can improve our online products and services. Other technologies that may be used with Digital Services include web beacons (which may operate in conjunction with cookies), Flash local stored objects and JavaScript. Some of these cookies and other technologies are consistent across our digital services, allowing us and the other providers of these services to understand you better and provide a more consistent experience across these services.

You can configure your web browser to reject and delete cookies and block JavaScript but you may limit functionality of our services. You can control your preferences regarding Flash local stored objects at

http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html

Our systems record a variety of information in relation to interactions with our Digital Services. This can include information about software versions used, device identifiers (like IP address), location data (where available and not disabled by the user), dates, times, file metadata, referring website, data entered and user activity such as links clicked.

In some instances, we may use third-party advertising companies to serve ads when you visit our websites. These companies may use information (not including your name, address, email address, or telephone number) about your visits to our websites and other websites in order to provide advertisements about goods and services of interest to you.

VII. Links

Our website may contain links to other websites operated by third parties. We make no representations or warranties in relation to the privacy practices of any third-party website and we are not responsible for the privacy policies or the content of any third party website. Third party websites are responsible for informing you about their own privacy practices.

VIII. Your Rights in Relation to Your Personal Information

Employees and agents of the Company are required to strictly respect and obey the rights of the Data Subjects. The Data Protection Officer and/or the Compliance Officer for Privacy (CoP), shall be responsible for monitoring such compliance and developing the appropriate disciplinary measures and mechanism.

1. RIGHT TO BE INFORMED

The Data Subject has the right to be informed whether Personal Data pertaining to him/her shall be, are being, or have been processed. Before entry of his/her Personal Data into the Company's Information and Communications Systems and/or Filing Systems, or at the next practicable opportunity, the Data Subject shall be notified and furnished with the following information:

1. Description of the personal information to be entered into the system;
2. purposes for which they are being or are to be processed;
3. scope and method of the personal information processing;
4. the recipients or classes of recipients to whom they are or may be disclosed;
5. methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
6. the identity and contact details of the personal information controller or its representative;
7. the period for which the information will be stored; and
8. the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

2. RIGHT TO OBJECT

The Data Subject shall have the right to object to the processing of his/her personal data. The Data Subject shall also be notified and given an opportunity to withhold his/her consent to the processing in case of changes or any amendment to the information supplied or declared to the Data Subject.

When a Data Subject objects or withholds consent, the Company shall no longer process the Personal Data, unless:

- The personal data is needed pursuant to a subpoena;
- the collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the data subject; or
- the information is being collected and processed as a result of a legal obligation.

3. RIGHT TO ACCESS

The Data Subject has the right to demand reasonable access to the following:

- Contents of his or her personal data that were processed;
- sources from which personal data were obtained;
- names and addresses of recipients of the personal data;
- manner by which such data were processed;
- reasons for the disclosure of the personal data to recipients, if any;
- information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject;
- date when his or her personal data concerning the data subject were last accessed and modified; and
- the designation, name or identity, and address of the personal information controller.

4. RIGHT TO CORRECTION

The Data Subject has the right to dispute the inaccuracy or error in the Personal Data Record and and may demand the Personal Information Controller ("PIC") to correct the erroneous information immediately unless such request appears to vexatious and/or otherwise unreasonable.

If the Personal Data has been corrected, the PIC shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients, thereof, provided, that recipients or third-parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification upon reasonable request of the data subject.

5. RIGHT TO ERASURE OR BLOCKING

The Data Subject shall have the right to suspend, withdraw and/or may request for the blocking, removal and/or destruction of his/her personal data from the Personal Information Controller's filing system.

1. This right may be exercised upon discovery and substantial proof of any of the following:

    a. The personal data is incomplete, erroneous, outdated, false, or was unlawfully obtained;
    b. the personal data is being used without the Data Subject's consent and/or for non- legitimate purpose/s;
    c. the personal data is no longer necessary for the purposes for which they were collected;
    d. the Data Subject has formally withdrawn his/her previously given consent and/or has objected to the processing of his/her personal information, and there is no legal basis to continue processing said information nor any overriding legitimate interest to justify the same;
    e. the information involved is prejudicial to the Data Subject and processing it would violate the Data Subject's fundamental rights and freedoms under the Constitution.

2. The PIC or PIP violated the rights of the Data Subject as found by the National Privacy Commission upon final judgment.

6. RIGHT TO DAMAGES

MicroSourcing shall indemnify the Data Subject for any loss and/or damage, if in the determination of the National Privacy Commission as sustained upon final judgment by the Highest Court, the Data Subject suffered loss and/or damage due to the Company's violation of its Privacy Policy and/or the Data Privacy Act of 2012.

7. RIGHT TO DATA PORTABILITY

Where the Data Subject's personal data is processed by electronic means and in a structured and commonly used format, he/she shall have the right to obtain from the personal information controller a copy of such data in an electronic or structured format that is commonly used and allows for further use by the data subject.

The exercise of this right shall primarily take into account the right of Data Subject to have control over his or her personal data being processed based on consent or contract, for commercial purpose, or through automated means. The Commission (NPC) may specify the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer.

8. RIGHT TO COMPLAIN BEFORE THE COMMISSION

The Data Subject shall have the right to complain before the National Privacy Commission for any privacy violation committed by the company, if any.

9. TRANSMISSIBILITY OF RIGHTS OF THE DATA SUBJECT

The lawful heirs and assigns of the Data Subject may invoke the rights of the latter to which he or she is an heir or an assignee, at any time after the death of the data subject, or when the Data Subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.

IX. Security of Your Personal Information

We take reasonable steps to ensure your personal information is protected from misuse and loss and from unauthorized access, modification or disclosure. We may hold your information either in electronic or hard copy form. Personal information is destroyed or de-identified when no longer required for any of the purposes for which it may be lawfully used or disclosed.

MicroSourcing keeps and protects information using a secured server behind a firewall, encryption technology and application of security controls. Access to personal information is restricted only to qualified and/or authorized personnel to hold said information with strict confidentiality. Conduct regular audit and rigorous testing of its infrastructure's security protocols to ensure that data is always protected. Updates the information securely to keep the records accurate.

The DPO, with the assistance of the COP/s, if any, and the Data Privacy Response Team, shall monitor the MicroSourcing compliance with the Security Measures specified in this Policy.

1. Organizational Security Measures

A. Data Privacy Principles

All Processing of Personal Data within the Company shall be conducted in compliance with the following data privacy principles as espoused in the Data Privacy Act.

- **Transparency**
  The Data Subject shall be informed of the nature, purposes, and extent of the Processing of his/her Personal Data, including the risks and safeguards involved, the identity of the Company, his/her rights as a Data Subject, and how these rights may be exercised.
- **Legitimate Purpose**
  The Processing of Personal Data shall only be for the purpose declared and specified to the Data Subject. No further Processing of Personal Data shall be done without the consent of the Data Subject.
- **Proportionality**
  The Processing of Personal Data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal Data shall be processed by the company only for legitimate, necessary and/or reasonable purposes.

2. Physical Security Measures

MicroSourcing shall ensure compliance with the Data Privacy Act of 2012 by following guidelines and appropriate physical security measures such as:

- Policies and procedures shall be implemented to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media;
- design of office space and work stations, including the physical arrangement of furniture and equipment shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public;
- the duties, responsibilities and schedule of individuals involved in the processing of personal data shall be clearly defined to ensure that only individuals actually performing official duties shall be in the room or work station, at any given time;
- any natural or juridical person or other body involved in the processing of personal data may implement policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of personal data;
- policies and procedures that prevent the mechanical destruction of files and equipment shall be established. The room and workstation used in the processing of personal data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

3. Technical Security Measures

The Company recognizes the need to implement 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. These security measures include the following, among others:

- Role of Data Privacy Office/DPO/Site leads, employees and contractors
- Minimum technical security policies and procedures:
  a. Access controls;
  b. monitoring for security incidents and personal data breaches;
  c. security features of the software/s and application/s used;
  d. process for regular testing, assessment and evaluation of effectiveness of security measures;
  e. backup, restoration and recovery of personal data;
  f. network security;
  g. encryption, authentication process, and other technical security measures that control and limit access to personal data.

X. Data Breach and Security Incidents

A. Data Breach Notification

All Employees, agents and representatives of the Company involved in the processing of Personal Data are tasked to regularly monitor for signs of possible data breach or security incident. In the event that such signs are discovered, the employee or agent shall immediately report the incident to the DPO within twenty-four (24) hours from discovery for verification as to whether or not a breach requiring notification, pursuant to the Data Privacy Act (DPA), has occurred and to determine the relevant circumstances surrounding such breach or incident. The DPO shall formally notify the National Privacy Commission and affected Data Subjects pursuant to the requirements and procedures prescribed by the DPA.

The notification to the National Privacy Commission and the affected Data Subject shall describe the nature of the breach, the Personal Data involved, and the measures taken by the Company to address the breach. The report shall also include measures taken to mitigate the harm or negative consequences of the breach and the name and contact details of the DPO. The form and procedure for notification shall conform to the regulations and circulars issued by the National Privacy Commission, which may be updated from time to time.

B. Breach Reports

All security incidents and personal data breaches shall be documented through written reports, including, but not limited to, those not covered by the reportorial requirement. In case of personal data breaches, a report shall also include the facts surrounding the incident; the actual and possible effects thereof; and the remedial actions taken by the Company. In other Security Incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation. These reports shall be made available when requested by the National Privacy Commission. A general summary of the reports shall be submitted annually by the DPO to the National Privacy Commission.

XI. Complaints

If you believe your personal information is not properly protected or that there has been a breach or potential breach of this Privacy Policy and/or the Data Privacy Act, we enjoin you to immediately notify MicroSourcing's Data Protection Officer (DPO).

As MicroSourcing takes breach incidents seriously, we have laid down procedures to help identify and resolve an actual and/or potential breach. This includes appropriate escalation processes to the Data Privacy Breach Response Team and notification processes in the event of a breach.

In the event of an actual and/or potential breach, the complaint shall be immediately forwarded to Data Protection Officer. You shall be notified about the progress and outcome of the investigation.

XII. Contacting Us

If you have any concerns and/or questions about our Privacy Policy or any complaint and/or grievance on the manner your personal information is being managed and/or handled, please use the contact link on our website and/or contact the Data Protection Officer through the contact details below:

DATA PROTECTION OFFICER: Bernadette Jean Frias
COMPANY NAME: MicroSourcing Philippines, Inc.
COMPANY ADDRESS: 2nd Floor, 1880 Building, Eastwood CyberPark Bagumbayan, Quezon City 1110
EMAIL ADDRESS: dpo@microsourcing.com
LANDLINE: +63 (0) 2 3 437 1000 loc. 9991
MOBILE NUMBER: +63 917 835 6044

Rest assured that we shall address your questions, concerns and/or complaint with utmost confidentiality. In case of a complaint, our authorized representative will contact you within forty-eight (48) hours upon receipt of your complaint to address and/or discuss your concerns.

XIII. References

- ISO 27001:2013
- ISO 9001:2015
- Data Privacy Act of 2012

XIV. Changes to Our Privacy Policy

MicroSourcing reserves the right to amend or update its Privacy Policy from time to time. You agree to be bound by the provisions of this Policy as published on our website. You may visit our website regularly for any updates regarding this Policy

This privacy policy was last updated on 01 July 2021.