



# Personal Data Privacy Policy

POLICY

**INTERNAL**

*This document has been security classified using the CNVRG's information security classification framework as **INTERNAL** and will be managed according to Converge ICT Solutions Inc.'s quality and information security governance and compliance requirements.*

**- MASTER COPY -**

**INTERNAL**

*This document has been security classified using the CNVRG's information security classification framework as **INTERNAL** and will be managed according to Converge ICT Solutions Inc.'s quality and information security governance and compliance requirements.*

**- MASTER COPY -**

## Table of Contents

1. Purpose of this policy .....	4
2. Scope of this policy .....	4
3. Definitions .....	4
4. Policy Statement .....	5
4.1. Governance .....	5
4.2. Risk Assessment .....	5
4.3. General Procedures in Upholding Data Subject Rights .....	6
4.4. Data Subject Rights .....	7
4.5. Limitation of Rights .....	13
4.6. Denial of Request .....	13
4.7. Reasonableness of the denial or limitation .....	14
4.8. Security Measures for the Protection of Personal Data .....	14
4.9. Data Breaches and Notification .....	16
4.10. Outsourcing and Subcontracting Agreements .....	16
5. Policy Compliance .....	17
5.1. Compliance Measurement .....	17
5.2. Non-compliance .....	17
6. Related document references .....	17
7. Details of revision/s made to this policy .....	17
8. Annexes .....	19

**INTERNAL**

*This document has been security classified using the CNVRG's information security classification framework as **INTERNAL** and will be managed according to Converge ICT Solutions Inc.'s quality and information security governance and compliance requirements.*

**- MASTER COPY -**

## 1. Purpose of this policy

The purpose of this policy is to adhere and comply with the requirement set forth in R.A. 10173 or commonly known as Data Privacy Act of 2012 “**Act**”, its Implementing Rules and Regulations “**IRR**”, and other relevant policies including issuances and notices of the National Privacy Commission “**NPC**”.

This policy will serve as a statement of Converge Information and Communications Technology Solutions, Inc. in protecting personal information, in implementing appropriate security measures, and in exercising the data subject’s rights under the Act.

## 2. Scope of this policy

This policy applies to all data processing activities, data processing systems or programs within CNVRG and individuals whose roles comprises of collecting, processing, sharing, disclosing and destroying personal information.

## 3. Definitions

- **Consent of Data Subject** – refers to refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so. (Section 3.b of DPA)
- **Data Subject** – refers to an individual whose personal, sensitive personal or privileged information is processed by the organization.
- **Information and Communications System** – refers to a system for generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or which data is recorded, transmitted or stored and any procedure related to the recording, transmission or storage of electronic data, electronic message, or electronic document. (Section 3.f of DPA)
- **Personal Information Controller (PIC)** – refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. (Section 3.h of DPA)
- **Personal Information Processor (PIP)** – refers to a person or organization to whom a personal information controller may outsource the processing of personal information. (Section 3.i of DPA)
- **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. (Section 3.j of DPA)
- **Personal Identifiable Information (PII)** – refers to any data that may be used (either alone with other relevant data) to identify a specific individual.
- **Sensitive Personal Information (SPI)** – refers to personal information about an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations. Any information about an individual’s health, education, genetic or sexual life, or any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings. Information issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns.
- Converge Information and Communications Technology Solutions, Inc will be referred to as “**CNVRG**”
- **Personal Data** – Personal Information, Sensitive Personal Information and Privileged Information collectively.
- **Company** – refers to CNVRG, its affiliates and subsidiaries collectively.

**INTERNAL**

*This document has been security classified using the CNVRG’s information security classification framework as **INTERNAL** and will be managed according to Converge ICT Solutions Inc.’s quality and information security governance and compliance requirements.*

**- MASTER COPY -**

## 4. Policy Statement

Company respects and values the privacy rights of the data subject, and ensures that all Personal Data collected from employees, clients, customers, third party vendors, and its affiliates are processed in adherence to the general principle of proportionality, transparency, and legitimate purpose.

All employees and personnel must comply with the requirements and guidelines set in this Policy and ensure that personal information of internal and external stakeholders is kept secure and protected.

### 4.1. Governance

- 4.1.1. In compliance with the Act, Company shall nominate, appoint or designate a Data Protection Officer “DPO”. The selected DPO shall be accountable for ensuring adherence with the data privacy laws and regulations for the protection of data privacy and security. [NPC Advisory No. 2017-01 – Designation of Data Protection Officers.](#)
- 4.1.2. The DPO’s functions and responsibilities particularly include, among others:
  - 4.1.2.1. continuous monitoring of Company’s Personal Data processing systems and activities in order to show its commitment and ensure compliance with applicable personal data privacy laws and regulations, including conduct of internal audits and reviews in periodic intervals to guarantee that data privacy policies are adequately implemented and adhered to by its authorized representatives and employees;
  - 4.1.2.2. act as liaison between Company and the regulatory accrediting bodies, and oversees appropriate registration, reportorial, and notification requirements as mandated by the Act, as well as other applicable data privacy laws and regulations;
  - 4.1.2.3. development, establishment, and review of data privacy policies and procedures to ensure that the data subject can exercise their rights under the Act;
  - 4.1.2.4. the point of contact whom the data subject can consult and coordinate for all data privacy concerns and inquiries relating to their personal data;
  - 4.1.2.5. conduct data privacy awareness training programs for all Company employees, representatives or agents of the Company regarding data privacy and information security policies;
  - 4.1.2.6. prepare and submit annual report of the summary of documented information security incidents and personal data breaches, as required under the Act, and compliance with other requirements or issuances provided by the Commission.

### 4.2. Risk Assessment

- 4.2.1. **Registration.** To demonstrate Company compliance with the Act, Company shall register all its data processing systems which will also assist the Commission and those involved in the processing of Personal Data in upholding the rights of the data subject. NPC Circular 17-01 - Registration of Data Processing and Notifications regarding Automated Decision-Making.
- 4.2.2. **Records of data processing activities and applications.** Company shall maintain records of all data processing activities within the Company that sufficiently describe its data processing system and identify the duties and responsibilities of employees or individuals who will have access to personal data. As stated in Section 26 – c. Records of Processing Activities in the IRR of the Act, records shall include:
  - 4.2.2.1. Information about the purpose of the processing, including any secondary uses of Personal Data intended for future processing or data sharing which may also be used for the following reasons:

**INTERNAL**

*This document has been security classified using the CNVRG’s information security classification framework as **INTERNAL** and will be managed according to Converge ICT Solutions Inc.’s quality and information security governance and compliance requirements.*

**- MASTER COPY -**

- 4.2.2.1.1. **Data Analytics** which is important because it helps Company to optimize its performances. Implementing it the Company's business model means that the Company can help reduce costs by identifying more efficient ways of doing business and by storing large amounts of data. Company shall also use data analytics to make better business decisions and help analyze customer trends and satisfaction, which can lead to new and better products and services.
  - 4.2.2.1.2. **Research Purposes and Abiding with the DOH-NPC Joint Memorandum Circular No. 2020-0002**, enabling use of Personal Data by healthcare professionals and researchers is important to improve the quality of health care and research effectiveness. At the same time, it is important to protect the employees/customer's privacy and to ensure that no harm is done to a employees/customer's Personal Data.
  - 4.2.2.2. A description of all categories of data subjects, Personal Data, and recipients of such personal data that will be involved in the processing;
  - 4.2.2.3. General information about the data flow within the Company, from the time of collection, processing, and retention, including the time limits for disposal or erasure of Personal Data;
  - 4.2.2.4. A general description of the organizational, physical, and technical security measures are in place;
  - 4.2.2.5. The name and contact details of the PIC and, where applicable, the joint controller, the its representative, and the compliance officer or Data Protection Officer "**DPO**", or any other individual or individuals accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security;
- 4.2.3. **Privacy Impact Assessment "PIA"**. CNVRG shall conduct Privacy Impact Assessments (PIA) to identify risks associated with processing of Personal Data in CNVRG's data processing system and activities.

### 4.3. General Procedures in Upholding Data Subject Rights

- 4.3.1. **Exercise of Rights.** These rights shall be exercised by the data subject himself or herself. The data subject may, however, authorize another person to facilitate the exercise of any of these rights on his or her behalf: provided, that the authorization is specific and supported by appropriate documents.
- 4.3.1. **Transmissibility of Rights.** The lawful heirs and assigns of the data subject may likewise exercise any of his or her rights, at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the same.
- 4.3.2. **Policies and procedures.** CNVRG shall establish policies and procedures allowing for the exercise of data subjects of their rights. The following shall be considered:
  - 4.3.2.1. **Request Form.** CNVRG shall ensure that the process is clear, simple, straightforward, and convenient, and should be sufficiently communicated to the data subjects. CNVRG adopted the standard forms shared by the NPC to act on data subject's request such as right to access, right to rectification and erasure, respectively. CNVRG may modify these forms if necessary or according to the needs and requirement of CNVRG. Refer to Section 8 of this document (Annex).
  - 4.3.2.1.1. **Verification of the identity of the requesting party.** CNVRG shall use reasonable measures to verify the identity of the requesting data subject. For this purpose, CNVRG may require the presentation of supporting documents to verify the identity of the requesting party, ensuring that the requested information is only to the extent necessary to confirm such identity.
    - a. For persons requesting for and on behalf of another, CNVRG may request for evidence of proper authorization and supporting documents to validate the authority and identity of the representative as well as to confirm the identity of the requesting party; and
    - b. For the legal heirs and assigns of the data subject invoking the transmissibility of the right of the data subject, CNVRG may require the following documents for verification purposes:

**INTERNAL**

*This document has been security classified using the CNVRG's information security classification framework as **INTERNAL** and will be managed according to Converge ICT Solutions Inc.'s quality and information security governance and compliance requirements.*

**- MASTER COPY -**

1. Death Certificate of the data subject;
  2. Birth Certificate of the legal heirs and assigns; and
  3. Other supporting documents to validate the authority and identity of the representative as well as to confirm the identity of the requesting party.
- c. For organizations requesting on behalf of its members, CNVRG may request for evidence on proper authorization, supporting documents to validate the membership of the data subject in the organization and the authority of the organization to file on behalf of the affected data subjects: provided, that all its members are affected data subjects.
- 4.3.1.2. **Assistance of PIPs.** CNVRG shall ensure, by contractual or other reasonable means, that the PIPs it has engaged to process personal data on its behalf shall cooperate and coordinate with CNVRG in addressing any requests for the exercise of data subject rights.
- 4.3.1.3. **Fees and Charges.** CNVRG shall not charge any fee to fulfill the exercise of data subject rights. As an exception, where data subjects request copies of their personal data and the other information in exercising their right to access, CNVRG may require reasonable fees to cover administrative costs: provided, that fees imposed shall not be so exorbitant or excessive as to have the effect of discouraging such requests.
- 4.3.1.4. **Reasonable period for complying with the request.** CNVRG Reasonable period for complying with the request (30) working days after receipt of the request and/or the necessary supporting or additional documentation: provided further, that if a request is complex or numerous, compliance with such request may be extended for a period not exceeding another fifteen (15) working days: provided finally, that the data subject or his or her authorized representative is notified of the reason for the extension.
- 4.3.1.5. **Retention.** CNVRG shall not retain personal data for the sole purpose of making it available for potential future requests for the right to access or data portability. Personal data shall be retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained.

## 4.4. Data Subject Rights

As provided under the Act, the data subjects have the following rights in connection with the processing of their Personal Data. CNVRG employees, its agents and representatives are duty bound to observe and respect every data subject's rights to privacy. The DPO, with the assistance of Corporate Human Resources and other relevant departments shall be responsible for monitoring the compliance and developing the appropriate disciplinary measures and mechanism.

### 4.4.1. Right to be Informed

- 4.4.1.1. The Data Subject has the right to be informed whether Personal Data pertaining to him or her shall be, are being, or have been processed.
- 4.4.1.2. The Data Subject shall be notified and furnished with information indicated hereunder before the entry of his or her Personal Data into the processing system of CNVRG, or at the next practical opportunity:
  - Description of the Personal Data to be entered into the system;
  - Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;
  - Basis of processing, when processing is not based on the consent of the data subject;
  - Scope and method of the Personal Data processing;
  - The recipients or classes of recipients to whom the personal data are or may be disclosed;

**INTERNAL**

*This document has been security classified using the CNVRG's information security classification framework as **INTERNAL** and will be managed according to Converge ICT Solutions Inc.'s quality and information security governance and compliance requirements.*

**- MASTER COPY -**

- Methods utilized for automated access, if the same is allowed by the Data Subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- The identity and contact details of the PIC or its representative;
- The period for which the information will be stored; and;
- The existence of their rights as Data Subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the NPC.

4.4.1.3. A privacy notice is an embodiment of the observance or demonstration of the data privacy principle of transparency and upholding the right to information of data subjects. It is a statement made to data subjects that describes how CNVRG collects, uses, retains, and discloses personal information. Information provided to a data subject must always be in clear and plain language to ensure that they are easy to understand and access:

- a. **Language.** Whether a privacy notice is communicated verbally or in writing, best practices for clear and plain language must be observed. This does not, however mean that the requirement to use clear and plain language necessitates using layman's terms in place of technical words at the risk of not capturing the complex concepts they represent. CNVRG should determine whether an average member of the target audience could have understood the information provided to them. Complex sentence structures and equivocal wordings that may be subject to different interpretations should be avoided.
- b. **Form.** The Act does not dictate the form and method of how CNVRG should inform its data subjects. Nonetheless, in crafting privacy notices, CNVRG should consider when it is provided, how it is delivered, how it is communicated, and how choices are provided. CNVRG may likewise consider adopting multilayered privacy notices which constitute a set of complementary privacy notices that are tailored to the respective audience and the contexts in which they are presented. The granularity of information provided in a specific notice layer must be appropriate for the respective context.

4.4.1.4. A privacy notice is not equivalent to consent. While consent may not be required in certain instances when it is not relied on as basis for processing personal data, a privacy notice is required at all times in order for data subjects to be informed of the processing of their personal data and their rights as data subjects.

#### 4.4.2. Right to Object

The Data Subject shall have the right to object to the processing of his or her Personal Data, including processing for direct marketing, automated processing, or profiling. The Data Subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the Data Subject in the preceding paragraph. When a Data Subject objects or withholds consent, the PIC shall no longer process the Personal Data, unless:

- a. Personal Data is needed pursuant to a subpoena;
- b. 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
- c. the information is being collected and processed as a result of a legal obligation.

In case of any significant change or amendment to the information provided to the data subject in a consent form, privacy notice, or similar communication, the data subject shall be notified and given an opportunity to object and/or withdraw consent, if consent was previously given for such personal data

**INTERNAL**

*This document has been security classified using the CNVRG's information security classification framework as **INTERNAL** and will be managed according to Converse ICT Solutions Inc.'s quality and information security governance and compliance requirements.*

**- MASTER COPY -**



processing. For this purpose, a significant change or amendment shall include the purpose/s of processing, scope and method of processing, and other analogous instances

4.3.1.1. Data subjects have the right to object to the processing of his or her personal data for direct marketing, profiling, or in cases of automated processing where the personal data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect him or her. For this purpose, data subjects shall be provided by CNVRG in clear and easy to understand language with adequate information on the effect of the exercise of this right vis-à-vis the provision of goods and/or services by CNVRG to the data subject. Said information that will be communicated to the data subjects should indicate the scope of the withdrawal of consent or objection and its consequences. This could mean removal of the personal data from the CNVRG's automated processing systems or its suppression in mailing/profiling lists in a way that it would not be processed for purposes that the data subject has objected to.

4.3.1.2. When a data subject objects, CNVRG shall cease the processing of personal data and comply with the objection, unless the processing falls under any other allowable instances pursuant to in Sections 12 or 13, other than consent and legitimate interest. Should there be other grounds to continue processing the personal data, CNVRG shall have the burden of determining and proving the appropriate lawful basis or compelling reason to continue such processing. CNVRG shall also communicate and inform the data subject of said lawful basis or compelling reason to continue processing.

#### 4.4.3. Right to Access

4.4.3.1. A data subject has the right to obtain confirmation on whether or not data relating to him or her are being processed, as well as information about any of the following::

- a. Contents of his or her personal information and categories of data that were processed;
- b. Sources from which personal information were obtained, if the data was not collected from the data subject;
- c. Purposes of processing;
- d. Manner by which such data were processed;
- e. Information on automated processes where the processed data will or is likely to be made as the sole basis for any decision that significantly affects or will affect the data subject;
- f. Names and addresses of recipients of the personal information;
- g. Reasons for the disclosure of the personal information to recipients;
- h. Date when his or her personal information were last accessed and modified;
- i. Period for which particular categories of information will be stored; and
- j. The designation, name or identity, and address of the PIC's data protection officer.

4.4.3.2. A data subject may only request to have access to his or her own personal data and the other information in the immediately preceding paragraph and not to the information relating to any another individual. This would likewise exclude any analysis made by the CNVRG with respect to a data subject's personal data, i.e. inferred, derived, modeled, or business-generated data.

4.4.3.3. The following instances, where applicable, may limit the right to access:

**INTERNAL**

*This document has been security classified using the CNVRG's information security classification framework as **INTERNAL** and will be managed according to Converge ICT Solutions Inc.'s quality and information security governance and compliance requirements.*

**- MASTER COPY -**

- a. **Publicly Available Information.** If an existing law or regulation requires CNVRG to make the personal data available to the public, CNVRG has the discretion on whether to comply with the request or to direct the requesting party to where such information may be found or accessed. However, access to the other information in Section 4.3.2.1. should still be provided to the data subject where that specific information is not publicly available.
- b. **Repeated Request.** CNVRG may decide not to comply with repeated, identical, or similar requests if such request for access has been previously granted unless a reasonable interval of time from the previous request has elapsed. The determination of what constitutes a reasonable interval of time shall depend on the nature of the request, considering any changes or updates in the personal data and/or the other information in Section 4.3.2.1. from the time of the previous request.
- c. **Request which will entail disproportionate effort.** After reasonable evaluation, if the request for access would result in a disproportionate amount of effort or resources, CNVRG may refuse to comply with the request. The determination of what constitutes disproportionate effort may be made on the basis of the particular circumstances of the request. Factors to consider may include the availability of the information, the need for extraordinary measures to retrieve the information, the purpose of the request, and the necessity and benefit of the requested information to the data subject.
- d. **Consideration of the safety of the data subject.** In exceptional cases and subject to any applicable ethical guidelines, limitations on the right to access may apply if, in the professional evaluation and determination of CNVRG, providing access to the requested information may cause serious harm to the physical, mental, or emotional health of the data subject.

#### 4.4.4. Right to Rectification

The Data Subject has the right to dispute the inaccuracy or error in the Personal Data and have CNVRG correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the Personal Data has been corrected, CNVRG 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.

4.4.4.1. If the personal data has been corrected, CNVRG shall:

- a. 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; and
- b. Inform the recipients or third parties who have previously received such personal data of its inaccuracy and its subsequent rectification, upon reasonable request of the data subject.

4.4.4.2. This right excludes instances where rectification or correction requires an order from a competent court, other pertinent government agencies, or otherwise covered by an official process under other applicable laws and regulations.

4.4.4.3. Considering the purpose/s of the processing, the data subject shall have the right to have incomplete personal data completed, including means of providing a supplementary statement.

4.4.4.4. The request for rectification may be denied if the same is manifestly unfounded, vexatious, or otherwise unreasonable. The determination of whether the request is manifestly unfounded, vexatious, or unreasonable may be made on the basis of the particular circumstances of the request. A request may be considered as such when it is made with no real purpose other than to harass, cause annoyance, or hamper the delivery and performance of service.

**INTERNAL**

*This document has been security classified using the CNVRG's information security classification framework as **INTERNAL** and will be managed according to Converge ICT Solutions Inc.'s quality and information security governance and compliance requirements.*

**- MASTER COPY -**

## 4.4.5. Right to Erasure or Blocking

4.4.5.1. The Data Subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her Personal Data from CNVRG's filing system. This right may be exercised upon discovery of substantial proof of any of the following:

- the Personal Data is incomplete, outdated, false, or unlawfully obtained;
- the Personal Data is being used for purpose not authorized by the Data Subject;
- the Personal Data is no longer necessary for the purposes for which they were collected;
- the Data Subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;
- the Personal Data concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
- the processing is unlawful;
- the PIC or PIP violated the rights of the Data Subject.

4.4.5.2. CNVRG should judiciously evaluate requests for the exercise of the right to erasure or blocking.

a. **Approval or Request.** When a request for erasure is made on any of the following grounds, CNVRG is directed to grant such request:

1. Unlawful processing;
2. Used for unauthorized purposes; or
3. Violation of Data Subject's rights.

b. **Denial of Request.** A request for erasure or blocking maybe denied, wholly or partly, when Personal Data is still necessary in any of the following instances.

1. Fulfillment of the purpose/s for which the data was obtained;
2. Compliance with a legal obligation which requires personal data processing;
3. Establishment, exercise, or defense of any legal crime.
4. Legitimate business purposes of CNVRG, or consistent with the applicable industry standard for personal data retention;
5. To appraise the public on matters that have an overriding public interest or concern taking into consideration the following factors:
  - i. constitutionally guaranteed rights and freedoms of speech, of expression, or of the press;
  - ii. whether or not the personal data pertains to a data subject who is a public figure; and
  - iii. other analogous considerations where personal data are processed in circumstances where data subjects can reasonably expect further processing.

**INTERNAL**

*This document has been security classified using the CNVRG's information security classification framework as **INTERNAL** and will be managed according to Converge ICT Solutions Inc.'s quality and information security governance and compliance requirements.*

**- MASTER COPY -**

6. As may be provided by any existing law, rules, and regulations.

4.4.5.3. CNVRG shall inform the recipients or third parties who have previously received such personal data of the fact of erasure. CNVRG shall likewise inform the data subject about such recipients of his or her personal data.

4.4.5.4. Where Personal Data that is the subject of a request for erasure is publicly available, i.e. online, reasonable and appropriate measures shall be taken by CNVRG to communicate with other PICs, including third party indexes, and request them to erase copies or remove or de-list search results or links to the pertinent personal data. In determining what is reasonable and appropriate, the available technology and the cost of implementation shall be considered.

4.4.5.5. Data subjects must be adequately informed of the consequences of the erasure of their personal data.

#### 4.4.6. **Right to Damages**

The data subjects have the right to be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of their personal data, taking into account any violation of his or her rights and freedoms as data subject.

4.4.6.1. When there is a perceived violation of his or her rights, the data subject may file a complaint with the NPC, in accordance with its Rules of Procedure governing all complaints filed before the Commission.

4.4.6.2. In cases where a data subject files a complaint for violation of his or her rights, and for any injury suffered as a result of the processing of his or her personal data, the Commission may award indemnity on the basis of the applicable provisions of the New Civil Code.

#### 4.4.7. **Transmissibility of Rights of the Data Subject**

The lawful heirs and assigns of the Data Subject may invoke the rights of the Data Subject 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.

#### 4.4.8. **Right to Data Portability**

Where a Data Subject's Personal Data is processed by electronic means and in a structured and commonly used format, the Data Subject shall have the right to obtain from CNVRG 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 consider 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. NPC may specify the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer.

4.4.8.1. For the exercise of this right, the following conditions must concur:

- a. Processing is based on consent or contract; and
- b. Personal data is processed by electronic means and in a structured and commonly used format.

4.4.8.2. Data portability shall be limited to the personal data concerning the data subject, and which he or she has provided to CNVRG:

- a. Data actively and knowingly provided by the data subject, i.e. name, address, age, username, etc.; and

**INTERNAL**

*This document has been security classified using the CNVRG's information security classification framework as **INTERNAL** and will be managed according to Converge ICT Solutions Inc.'s quality and information security governance and compliance requirements.*

**- MASTER COPY -**

- b. Observed data provided by the data subject by virtue of the use of the service or the device, i.e. access logs, transaction history, location data, etc.
- 4.4.8.3. The exercise of this right shall not adversely affect the rights and freedoms of others. CNVRG, whether sending or receiving, should consider implementing security measures to reduce the risk for personal data of third parties to be included in the porting request. When ported data includes the data of other individuals, i.e. names and contact details within the contact directory of the requesting party, receiving party are prohibited from further processing such data for its own purpose, i.e. marketing, etc.
- 4.4.8.4. CNVRG shall consider using commonly used, machine-readable, interoperable, open formats, i.e. XML, JSON, CSV, etc. for data portability requests.

## 4.5. Limitation of Rights

- 4.5.1. **Limitations.** The exercise of the rights of data subjects shall be reasonable. The same may be limited when necessary for public interest, protection of other fundamental rights, or when the processing of personal data is for the following purposes:
- a. Scientific and statistical research: provided, that:
    - 1. No activities are carried out and no decisions are taken regarding the data subject;
    - 2. The personal data shall be held under strict confidentiality and shall be used only for research purpose; and
    - 3. Any research undertaken shall be subject to the applicable ethical and legal standards and processes, including but not limited to the submission of the research protocol to a recognized research ethics committee or ethics review board to ensure that ethical standards are observed.
  - b. Investigations in relation to any criminal, administrative, or tax liabilities of a data subject: provided, that:
    - 1. The investigation is being conducted by persons or entities duly authorized by law or regulation;
    - 2. The investigation or any stage thereof relates to any criminal, administrative, or tax liabilities of a data subject as may be defined under existing laws and regulations; and
    - 3. The limitation applies to the extent that complying with the requirements of upholding data subject rights would prevent, impair, or otherwise prejudice the investigation.
  - c. In the interest of national security, rights of data subjects may be limited pursuant to laws, rules and regulations, or order of a competent court.
  - d. Limitations on the exercise of data subject rights may be applied to analogous cases where the PIC has a legitimate purpose justifying such limitation. In all cases, limitations shall be proportional to the purpose of such limitation.

## 4.6. Denial of Request

- 4.6.1. In the event CNVRG denied a request or limits the exercise of the rights of data subjects, CNVRG shall ensure that the data subject is clearly and fully informed of the reason for the limitation or denial.

**INTERNAL**

*This document has been security classified using the CNVRG's information security classification framework as **INTERNAL** and will be managed according to Converge ICT Solutions Inc.'s quality and information security governance and compliance requirements.*

**- MASTER COPY -**

## 4.7. Reasonableness of the denial or limitation

- 4.7.1. The determination of the reasonableness of the limitation on or the denial of the exercise of data subject rights shall be made by the NPC upon the filing of a complaint by the data subject pursuant to the NPC's Rules of Procedure.

## 4.8. Security Measures for the Protection of Personal Data

In Rule VI of the IRR states that CNVRG as a PIC shall implement reasonable, appropriate, and practicable organizational, physical and technical security measures for the protection of personal information. These security measures shall aim to maintain the confidentiality, integrity and availability (CIA) of Personal Data and to protect data against unauthorized access, unlawful destruction, fraudulent misuse, alteration, disclosure, and unlawful processing.

### 4.8.1. Organizational Security Measures

- 4.8.1.1. **Data Privacy Principles.** All data processing activities and systems within CNVRG shall comply with the following data privacy principles as described in Rule IV – Data Privacy Principles of the IRR:

4.8.1.1.1. **Transparency.** The Data Subject must be aware of the nature, purpose, and extent of processing of his or her Personal Data, including the risks and safeguards involved, the identity of PIC, his or her rights as a Data Subject, and how these can be exercised. Any information and communication relating to the processing of Personal Data should be easy to access and understand, using clear and plain language.

4.8.1.1.2. **Legitimate Purpose.** The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.

4.8.1.1.3. **Proportionality.** The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal Data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

- 4.8.1.2. **Processing of Personal Data.** CNVRG shall develop and implement process and procedures:

- **Collection** – for the collection of Personal Data, including procedures for obtaining **consent**, when applicable;
- **Use** – to limit the processing of Personal Data, to ensure that it is only to the extent necessary for the declared, specified, and legitimate purpose;
- **Use** – to ensure that Data Subjects can exercise their rights under the Act;
- **Organization and storage** – for access management, system monitoring, and protocols to follow during security incidents or technical problems;
- **Sharing** – for the sharing of Personal Data with partners for legitimate business purpose, including procedures for obtaining consent, when applicable; and
- **Retention and disposal** – for records or data retention schedule, including timeline and conditions of erasure, destruction and disposal of records.

- 4.8.1.3. **Management of Human Resources.** The DPO, with the cooperation of CNVRG's Human Resources Department, must develop and implement security measures to ensure that all Company employees, agents or representatives who have access to Personal Data shall strictly process such information in compliance with the requirements set forth in the Act, its IRR, notices and issuances of NPC, as well as other applicable data protection laws. These measures may include drafting of new or updating existing relevant policies of CNVRG and conducting awareness training programs to educate its employees, agents and representatives on data privacy and information security. The Human Resource Department

**INTERNAL**

*This document has been security classified using the CNVRG's information security classification framework as **INTERNAL** and will be managed according to Converse ICT Solutions Inc.'s quality and information security governance and compliance requirements.*

**- MASTER COPY -**

shall aid the DPO in ensuring informed consent are obtained from employees, agents or representatives, evidence by written, electronic or recorded means:

- 4.8.1.3.1. the processing of the employee's Personal Data is for documentation and reportorial purposes; and
- 4.8.1.3.2. an obligation of confidentiality on the employee's part in connection with the Personal Data that he or she may encounter during the period of employment with CNVRG. This obligation shall still apply even after termination of contract, dismissal, and voluntary or involuntary resignation.
- 4.8.1.4. **Contracts with PIP or Third-Party.** CNVRG must ensure that all PIPs, Third-Party or Vendors who collect and process Personal Information on the Company's behalf shall ensure, where applicable, to implement strict security measures in adherence with the Act. CNVRG shall only engage and on-board PIPs, Third-Party or Vendors that provide guarantee to implement sufficient and proper security measures in compliance with the Act and ensure protection of the Data Subject's rights. Contracts with PIP's, Third-Parties, and Vendors who collect and process Personal Information must include a signed Non-Disclosure Agreement (NDA) and Data Sharing Agreement, as applicable.
- 4.8.2. **Physical Security Measures.** The DPO with the assistance from Human Resource and other relevant departments such as Information Technology, Information Security and Internal Security, shall develop and implement appropriate data privacy and information security policies and procedures to:
  - 4.8.2.1. monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of access to electronic media;
  - 4.8.2.2. manage the design of office space and workstations, including physical arrangement of furniture and equipment, in order to provide privacy to anyone processing Personal Data, taking into consideration the environment and accessibility to the public;
  - 4.8.2.3. ensure that duties, responsibilities and schedule of individuals involved in the processing of Personal Data shall be clearly defined to guarantee that only authorized persons performing official duties shall be in the room or workstation at any given time;
  - 4.8.2.4. ensure appropriate protection of Personal Data during transfer, removal, destruction, disposal and re-use of electronic media; and
  - 4.8.2.5. prevent mechanical destruction of files and equipment, and to secure against natural disasters, power disturbances, external access and other similar threats.
- 4.8.3. **Technical Security Measures.** The DPO with the assistance from Information Technology and Information Security Departments shall develop and implement appropriate data privacy and information security policies and procedures to:
  - 4.8.3.1. ensure protection of Company's computer network and systems against accidental or unlawful destruction, unauthorized access, misuse of company assets, and any interference that may affect data integrity or hinder the functioning or availability of the system, and may lead to unauthorized access through an electronic network;
  - 4.8.3.2. ensure and maintain the confidentiality, integrity, availability, and resilience of data processing systems and services;
  - 4.8.3.3. regularly monitor security breaches, create a process for both identifying and accessing reasonably foreseeable vulnerabilities in the Company's computer networks, and take preventive, corrective, and mitigating actions against information security incidents that can lead to a personal data breach;
  - 4.8.3.4. restore the availability and access to Personal Data in a timely manner in the event of physical or technical incident;
  - 4.8.3.5. regularly test, assess and evaluate the effectiveness of implemented security measures; and

**INTERNAL**

*This document has been security classified using the CNVRG's information security classification framework as **INTERNAL** and will be managed according to Converge ICT Solutions Inc.'s quality and information security governance and compliance requirements.*

**- MASTER COPY -**

- 4.8.3.6. encrypt personal data during storage and while in transit, and create a process for user authentication and other technical security measures that control and limit access thereto.

## 4.9. Data Breaches and Notification

- 4.9.1. **Data Breach Notification.** All Company employees who are involved in the processing of Personal Data are required to regularly monitor signs of a possible data breaches or an information security incidents. If there is a reasonable belief or upon knowledge of such data breach or information security incident, all Company employees are mandated to immediately report the facts and circumstances to the DPO, Data Privacy Manager or COP within twenty-four (24) hours from discovery. The DPO and Data Privacy Manager shall determine the scope, impact and nature of the breach and if it requires notification to the NPC and the affected Data Subjects pursuant to the requirements and procedures prescribed by the Act.

The NPC and the affected Data Subjects shall be notified and at least describe the nature of the personal data breach, PII or SPI involved, and the measures taken by CNVRG to address the breach. The notification should also include CNVRG's actions taken to reduce the harm or negative impact of the breach together with the name of the designated DPO. The form and procedure of the notification shall conform to the rules and regulations as well as circulars, advisories and issuances of the NPC.

- 4.9.2. **Breach Reporting.** CNVRG shall document all information security incidents and data breaches through written reports, including those not covered by the notification requirements. In case of personal data breaches, the report shall include the facts surrounding the incident, its impact, harm to Data Subjects, nature and scope of the breach, possible fines and penalties, and remedial actions taken by CNVRG. In other information security incidents not involving Personal Data, a report containing aggregated information shall constitute sufficient documentation. These reports shall be made available when requested by the NPC. Annually the DPO is required to submit an Annual Information Security Incident and Data Breaches to the NPC.

## 4.10. Outsourcing and Subcontracting Agreements

- 4.10.1. CNVRG may subcontract or outsource the processing of Personal Data: Provided, that the external entity or Third Party Service Provider shall use contractual or other reasonable means to ensure that proper safeguards are in place, to ensure the confidentiality, integrity and availability of the Personal Data processed, prevent its use for unauthorized purposes, and generally comply with the requirements of the Act, its IRR, other applicable data protection laws in processing Personal Data, and other issuances or notices of the NPC. The processing of Personal Data by an external entity or Third-Party Service Provider in behalf of CNVRG shall be governed by a contract or other legal act that binds the external entity or Third-Party Service Provider to CNVRG.
- 4.10.2. Such contract should expressly set out the subject matter, longevity and duration of the Personal Data processing, its nature and purpose, the type of Personal Data and categories of Data Subjects, CNVRG's rights and obligations, as well as the geographic location of the processing under agreement or contract.
- 4.10.3. The external entity or Third-Party Service Provider who entered into such contract with CNVRG does not give these external entities the authority to subcontract to another Third-Party Vendor the whole or part of the arrangement or service, unless expressly stipulated in writing in the same contract or supported by a separate written consent or agreement of CNVRG. The subcontracting agreement shall indicate that the PIP shall:
- 4.10.3.1. process the Personal Data only upon the documented instructions of CNVRG, including transfers of Personal Data to another country or an international organization, unless such transfer is required by law;
  - 4.10.3.2. ensure that an obligation of confidentiality is imposed on persons authorized to process the Personal Data;
  - 4.10.3.3. implement appropriate security measures and comply with the Act, its IRR, and other issuances and notices of the NPC;

**INTERNAL**

*This document has been security classified using the CNVRG's information security classification framework as **INTERNAL** and will be managed according to Converge ICT Solutions Inc.'s quality and information security governance and compliance requirements.*

**- MASTER COPY -**



- 4.10.3.4. not engage in any other external entity or vendor without prior instruction from CNVRG: provided, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking the account of the nature of processing;
- 4.10.3.5. assist CNVRG, by appropriate technical and organizational measures and to extent possible, fulfill the obligation to respond to the request of Data Subjects relative to the exercise of their rights;
- 4.10.3.6. assist CNVRG in ensuring compliance with the Act, its IRR, other relevant data protection laws, and other issuances or notices of the NPC, considering the nature of processing and the information available to the PIP;
- 4.10.3.7. at the choice of CNVRG, delete or return all Personal Data to CNVRG after the end of the provision of services relating to the processing: Provided, that this includes deleting existing copies unless storage is authorized by the Act or another law;
- 4.10.3.8. make available to CNVRG all information necessary to demonstrate compliance with the obligations laid down in the Act, and allow for and contribute to audits, including inspections, conducted by CNVRG or another auditor mandated by the latter;
- 4.10.3.9. immediately inform CNVRG if, in its opinion, an instruction infringes the Act, its IRR, or any other issuance of the NPC.

## 5. Policy Compliance

### 5.1. Compliance Measurement

The Data Privacy Team will verify the compliance of this policy through various methods, including but not limited to, business tool reports, internal or external audits, reviews and feedback to the policy owner.

### 5.2. Non-compliance

All Company process owners, department heads, and employees who is responsible or delegated to support the activity shall assist Data Privacy Team to properly conduct Privacy Impact Assessments.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Additionally, the Company may at its discretion seek legal remedies for damages incurred as a result of any violation. The company may also be required by law to report certain illegal activities to the proper enforcement agencies.

## 6. Related document references

- Data Privacy Act of 2012 or R.A. 10173
- Implementing Rules and Regulations of the Data Privacy Act of 2012
- NPC Advisory No. 2017-01 – Designation of Data Protection Officers
- Employee Code of Conduct
- NPC Advisory 2021-01

## 7. Details of revision/s made to this policy

From time to time the organization may make changes to this Policy and relevant Guidelines to improve the effectiveness of its operation.

**INTERNAL**

*This document has been security classified using the CNVRG's information security classification framework as **INTERNAL** and will be managed according to Converge ICT Solutions Inc.'s quality and information security governance and compliance requirements.*

**- MASTER COPY -**









Version No.	Date	Description of Change	Author	Approver
1.0	March 1, 2019	Privacy Policy (Draft)	Eumir Espiritu	Jojo Dionaldo
1.1	March 11, 2021	<ul style="list-style-type: none"><li>Updated signatories and relevant terms</li><li>Updated the Annex to reflect the revisions made on the documents</li></ul>	Eumir Espiritu	Ulysses Naguit

**INTERNAL**

*This document has been security classified using the CNVRG's information security classification framework as **INTERNAL** and will be managed according to Converge ICT Solutions Inc.'s quality and information security governance and compliance requirements.*

**- MASTER COPY -**

## 8. Annexes

Document No.	Document Name	File
MAN-IT-DP-001	Data Privacy Manual	 MAN-IT-DP-001 Data Privacy Manual
	Privacy Notice	<a href="#">Privacy Notice</a>
POL-IT-DP-002 Data Breach Management Policy	Data Breach Management Policy	 POL-IT-DP-002 Data Breach Management
	Privacy Impact Assessment Template	 PIA Questionnaire Template.xlsx
	Data Sharing Agreement Template	 Data Sharing Agreement Template
FRM-IT-DP-001	Access Request Form	 FRM-IT-DP-001 Access Request Form
FRM-IT-DP-002	Rectification Request Form	 FRM-IT-DP-002 Rectification Request
FRM-IT-DP-003	Erasure Request Form	 FRM-IT-DP-003 Erasure Request Form
	NDA – for vendors	 NDA Draft Format Vendor Manager

**INTERNAL**

This document has been security classified using the CNVRG's information security classification framework as **INTERNAL** and will be managed according to Converge ICT Solutions Inc.'s quality and information security governance and compliance requirements.

**- MASTER COPY -**