Republic of the Philippines
NATIONAL PRIVACY COMMISSION

NPC Advisory No. 2021 - 01

DATE : 29 January 2021

SUBJECT : DATA SUBJECT RIGHTS

WHEREAS, the right to privacy, which includes information privacy, is constitutionally protected and accorded recognition independent of its identification with liberty, and at the same time, Article II, Section 11 of the Constitution emphasizes that the State values the dignity of every human person and guarantees full respect for human rights;

WHEREAS, the Data Privacy Act of 2012 (DPA), provides that it is the policy of the State to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth;[1]

WHEREAS, the DPA provides that personal information must be collected for specified and legitimate purposes, processed fairly and lawfully, accurate, relevant and, where necessary, kept up to date, adequate and not excessive in relation to the purposes for processing, and retained only for as long as necessary;[2]

WHEREAS, the DPA and its Implementing Rules and Regulations (IRR) provide for the rights of the data subjects, instances where these may be duly exercised, and the obligations of personal information controllers and processors;[3]

WHEREAS, the DPA mandates that any doubt in the interpretation of any provision of the law shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed;[4]

WHEREFORE, in consideration of the foregoing premises, the National Privacy Commission (NPC) hereby issues this Advisory on the Rights of Data Subjects relevant to the processing of their personal data.

General Provisions

SECTION 1. ***Scope***. — This Advisory shall apply to all natural or juridical persons, or any other body in the government or private sector engaged in the processing of personal data within and outside of the Philippines, subject to the applicable provisions of the DPA, its IRR,

[1] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012), § 2.
[2] Data Privacy Act of 2012, § 11.
[3] Data Privacy Act of 2012, § 16-18.
[4] Data Privacy Act of 2012, § 38; Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 34-36.

and issuances by the NPC.

SECTION 2. ***General Principles***. — This Advisory is governed by the following principles:

A. The right to data privacy refers to the right empowering individuals to have reasonable control over the flow of their personal data;

B. The exercise of data subject rights is a demonstration that an individual takes control over his or her own personal data. Data subjects may exercise their rights under the DPA with due consideration of the rights and freedoms of others;

C. Personal information controllers (PICs) and processors (PIPs) shall uphold these rights, subject to limitations as may be provided for by law, and implement mechanisms which enable the free exercise of the same through procedures which are clear, simple, straightforward, and convenient; and

D. The free exercise of data subject rights is an indication that PICs and PIPs adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality, and demonstrate compliance and accountability in personal data processing.

General policies and procedures in upholding data subject rights

SECTION 3. ***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.

SECTION 4. ***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.

SECTION 5. ***Policies and procedures***. — PICs shall establish policies and procedures allowing for the exercise of data subjects of their rights. The following shall be considered:

A. *Request form.* There is no standard form or template. PICs shall, however, ensure that the process is clear, simple, straightforward, and convenient, and should be sufficiently communicated to the data subjects. PICs may adopt a standard form: *provided,* that any request containing information sufficient to process such request should be acted upon even if a standard form is not used.

   Refer to Annexes A, B, and C for the sample forms for the right to access, rectification, and erasure, respectively, which may be modified according to the needs of PICs.

B. *Verification of the identity of the requesting party.* The PIC shall use reasonable measures to verify the identity of the requesting data subject. For this purpose, the PIC 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.

1. For persons requesting for and on behalf of another, the PIC 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

2. For the legal heirs and assigns of the data subject invoking the transmissibility of the right of the data subject, the PIC may require the following documents for verification purposes:

    a) Death Certificate of the data subject;
    b) Birth Certificate of the legal heirs and assigns; and
    c) Other supporting documents to validate the authority and identity of the representative as well as to confirm the identity of the requesting party.

3. For organizations requesting on behalf of its members, the PIC 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.[5]

C. *Assistance of PIPs.* PICs 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 the PIC in addressing any requests for the exercise of data subject rights.

D. *Fees and charges.* Generally, PICs 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, the PIC 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.

E. *Reasonable period for complying with the request.* The PIC must comply with requests without undue delay: *provided,* that the period will not exceed thirty (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.

    For government agencies, the pertinent provisions of Republic Act No. 11032 or the Ease of Doing Business and Efficient Government Service Delivery Act of 2018 and its Implementing Rules and Regulations shall apply in responding and complying with requests of data subjects.

F. *Retention.* PICs 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.

[5] *See* MNLCI v. Pieceland Corporation, et al., NPC Case No. 190258 (2020) where a religious organization filed a case on behalf of all of its members whose rights where violated.

Rights of a Data Subject

SECTION 6. ***Right to be Informed.*** **—** 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, including the existence of automated decision-making and profiling.

A. PICs shall notify and furnish data subjects with information indicated below before their personal data is processed, or at the next practical opportunity:

   1. Description of the personal data to be entered into the system;

   2. Purposes for which they are being or will be processed, including processing for direct marketing, profiling, or historical, statistical, or scientific purpose;

   3. Basis of processing, when processing is not based on the consent of the data subject;

   4. Scope and method of the personal data processing;

   5. The recipients or classes of recipients to whom the personal data are or may be disclosed;

   6. 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;

   7. The identity and contact details of the personal information controller and its representative;

   8. The period for which the information will be stored or retained; and

   9. The existence of their rights as data subjects.

B. The "next practical opportunity" depends upon the surrounding circumstance of the case. However, the timing of the provision of information must always be within a reasonable period to give effect to the data subject's right to be informed.[6]

C. 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 the organization collects, uses, retains, and discloses personal information.[7]

   Information provided to a data subject must always be in clear and plain language to ensure that they are easy to understand and access.

   1. *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,

[6] See: ECA v. XXX, NPC Case No. 18-103 (2020).
[7] See: National Privacy Commission, NPC Advisory Opinion 2018- 013 (2018).

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. PICs 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.[8]

2. *Form.* The DPA does not dictate the form and method of how PICs should inform its data subjects. Nonetheless, in crafting privacy notices, PICs should consider when it is provided, how it is delivered, how it is communicated, and how choices are provided. PICs 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.[9]

D. 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.

SECTION 7. ***Right to Object.*** **—** The data subject shall have the right to object to the processing of his or her personal data where such processing is based on consent or legitimate interest.[10]

A. 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 processing.

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

B. 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 PICs 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 the PIC to the data subject. Said information that will be communicated to the data subjects should indicate the

[8] See JVA v. U-PESO.PH LENDING CORPORATION (UPESO), NPC Case No. 19-498 (2020).
[9] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor, *A design space for effective privacy notices,* In Proceedings of the Symposium on Usable Privacy and Security (SOUPS'15), *available at* https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf (2015) (last accessed 15 Jan 2021).
[10] When processing is based on consent, the right to object is inherent since consent, by its nature and definition, may be withdrawn. As to processing based on legitimate interest, the right to object applies when the rights and freedoms of the data subject overrides such legitimate interest of the PIC or of a third party. For instance, a data subject can invoke his or her right to object where personal data are processed in circumstances where he or she does not reasonably expect further processing or when the processing is causing substantial damage or distress to the data subject.

scope of the withdrawal of consent or objection and its consequences. This could mean removal of the personal data from the PIC'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.

C. When a data subject objects, the PIC 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, the PIC shall have the burden of determining and proving the appropriate lawful basis or compelling reason to continue such processing. The PIC shall communicate and inform the data subject of said lawful basis or compelling reason to continue processing.

SECTION 8. ***Right to Access.*** **—** The right of data subjects to access information on the processing of their personal data shall be subject to the following guidelines:

A. 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:

   1. Contents of his or her personal information and categories of data that were processed;
   2. Sources from which personal information were obtained, if the data was not collected from the data subject;
   3. Purposes of processing;
   4. Manner by which such data were processed;
   5. 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;
   6. Names and addresses of recipients of the personal information;
   7. Reasons for the disclosure of the personal information to recipients;
   8. Date when his or her personal information were last accessed and modified;
   9. Period for which particular categories of information will be stored; and
   10. The designation, name or identity, and address of the PIC's data protection officer.

B. 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 PIC with respect to a data subject's personal data, i.e. inferred, derived, modeled, or business-generated data.

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

   1. *Publicly available information.* If an existing law or regulation requires PICs to make the personal data available to the public, the PIC 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 8(A) should still be provided to the data subject where that specific information is not publicly available.

2. *Repeated requests.* The PIC 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 8(A) from the time of the previous request.

3. *Requests which will entail disproportionate effort.* After reasonable evaluation, if the request for access would result in a disproportionate amount of effort or resources, the PIC 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.

4. *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 the PIC, providing access to the requested information may cause serious harm to the physical, mental, or emotional health of the data subject.

SECTION 9. *Right to Rectification.* — The data subject has the right to dispute the inaccuracy or error in his or her personal data and have the PIC correct the same within a reasonable period of time.

A. If the personal data has been corrected, the PIC shall:

   1. 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
   2. 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.

B. 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.

C. 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.

D. 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.

SECTION 10. ***Right to Erasure or Blocking.*** **—** A data subject has the right to request for the suspension, withdrawal, blocking, removal, or destruction of his or her personal data from the PIC's filing system, in both live and back-up systems.

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

   1. The personal data is:
      a) incomplete, outdated, false, or unlawfully obtained;
      b) used for an unauthorized purpose;
      c) no longer necessary for the purpose/s for which they were collected; or
      d) concerns private information that is prejudicial to the data subject, unless justified by freedom of speech, of expression, or of the press, or otherwise authorized;

   2. The data subject objects to the processing, and there are no other applicable lawful criteria for processing;

   3. The processing is unlawful; or

   4. The PIC or PIP violated the rights of the data subject.

B. PICs should judiciously evaluate requests for the exercise of the right to erasure or blocking.

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

      a) Unlawful processing;
      b) Used for unauthorized purposes; or
      c) Violation of data subject rights

   2. *Denial of Request.* A request for erasure or blocking may be denied, wholly or partly, when personal data is still necessary in any of the following instances:

      a) Fulfillment of the purpose/s for which the data was obtained;
      b) Compliance with a legal obligation which requires personal data processing;
      c) Establishment, exercise, or defense of any legal claim;
      d) Legitimate business purposes of the PIC, consistent with the applicable industry standard for personal data retention;
      e) To apprise 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.

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

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

D. 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 the PIC 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.

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

Section 11. ***Right to Data Portability.*** **—** The data subject shall have the right to obtain from the PIC a copy of his or her personal data and/or have the same transmitted from one PIC to another, in an electronic or structured format that is commonly used and allows further use by the data subject.

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

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

B. Data portability shall be limited to the personal data concerning the data subject, and which he or she has provided to the PIC:[11]

1. Data actively and knowingly provided by the data subject, i.e. name, address, age, username, etc.; and
2. 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.

C. The exercise of this right shall not adversely affect the rights and freedoms of others. PICs, 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 PICs are prohibited from further processing such data for its own purpose, i.e. marketing, etc.[12]

D. PICs shall consider using commonly used, machine-readable, interoperable, open formats, i.e. XML, JSON, CSV, etc. for data portability requests.

---

[11] See: European Commission, Article 29 Data Protection Working Party, Guidelines on the right to data portability, Adopted on 13 December 2016 As last Revised and adopted on 5 April 2017, available at https://webcache.googleusercontent.com/search?q=cache:N9BoIYGlK6UJ:https://ec.europa.eu/newsroom/document.cfm%3Fdoc_id%3D44099+&cd=1&hl=en&ct=clnk&gl=ph (last accessed: 6 October 2020).

[12] *Id.*

Section 12. ***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.

A. 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.

B. 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.

Limitation on Rights

SECTION 13. ***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.

SECTION 14. ***Denial of request.*** **—** Where a PIC denies or limits the exercise of data subject

rights, the PIC should ensure that the data subject is clearly and fully informed of the reason for the limitation or denial.

SECTION 15. ***Reasonableness of the denial or limitation.*** **—** 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.

SECTION 16. ***Interpretation.*** **—** Any doubt in the reasonableness of denying or limiting the exercise of data subject rights shall be liberally interpreted in a manner that would uphold the rights and interests of the data subject.

Approved:

SGD.
RAYMUND E. LIBORO
Privacy Commissioner

SGD.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

SGD.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

ANNEX A*

ACCESS REQUEST FORM

(NAME OF PERSONAL INFORMATION CONTROLLER)

I. DATA SUBJECT INFORMATION

FULL NAME	
ADDRESS	
EMAIL ADDRESS	**MOBILE NUMBER**

II. INFORMATION REQUESTED

- ☐ Contents of his or her personal information and categories of data that were processed
- ☐ Sources from which personal information were obtained, if data was not collected from the data subject
- ☐ Purposes of processing
- ☐ Manner by which such data were processed
- ☐ 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
- ☐ Names and addresses of recipients of the personal information
- ☐ Reasons for the disclosure of personal information to recipients
- ☐ Date when his or her personal information were last accessed and modified
- ☐ Period for which particular categories of information will be stored
- ☐ Designation, name or identity, and address of the PIC's data protection officer
- ☐ Others, please specify details:

III. RELEASE OF THE REQUESTED INFORMATION

☐ Electronic mail ☐ Hardcopy ☐ Others *(please specify)* _____

IV. DECLARATION

I declare that this form is accomplished by the undersigned and is a true, correct, and complete statement of the information contained herein. I also authorize (NAME OF PERSONAL INFORMATION CONTROLLER) to verify/validate the contents stated herein.

_____

SIGNATURE OVER PRINTED NAME

V. AUTHORIZED REPRESENTATIVES

FULL NAME	
ADDRESS	
EMAIL ADDRESS	**MOBILE NUMBER**

I declare that this form is accomplished by the undersigned as the authorized representative of the data subject. It is a true, correct, and complete statement of the information contained herein. Enclosed is the proof of the authority to act on of behalf of the data subject. I authorize (NAME OF PERSONAL INFORMATION CONTROLLER) to verify/validate the contents stated herein.

SIGNATURE OVER PRINTED NAME

FOR INTERNAL USE ONLY	
RECEIVED BY:	**REMARKS:**
DATE RECEIVED:	

**** PICs shall only require information that is necessary to the request and to confirm the identity of the requesting individual or his/her authorized representative, taking into consideration the principle of proportionality.***

ANNEX B*

RECTIFICATION REQUEST FORM

(NAME OF PERSONAL INFORMATION CONTROLLER)

I. DATA SUBJECT INFORMATION

FULL NAME	
ADDRESS	
EMAIL ADDRESS	**MOBILE NUMBER**

II. DETAILS OF REQUEST

INACCURATE/ERRONEOUS INFORMATION *(Please provide sufficient details. Use separate sheet if necessary.)*	**CORRECT INFORMATION** *(Please provide documentation, where necessary and appropriate)*

III. DECLARATION

I declare that this form is accomplished by the undersigned and is a true, correct, and complete statement of the information contained herein. I also authorize (NAME OF PERSONAL INFORMATION CONTROLLER) to verify/validate the contents stated herein.

SIGNATURE OVER PRINTED NAME

IV. AUTHORIZED REPRESENTATIVES

FULL NAME	
ADDRESS	
EMAIL ADDRESS	**MOBILE NUMBER**

I declare that this form is accomplished by the undersigned as the authorized representative of the data subject. It is a true, correct, and complete statement of the information contained herein. Enclosed is the proof of the authority to act on of behalf of the data subject. I authorize (NAME OF PERSONAL INFORMATION CONTROLLER) to verify/validate the contents stated herein.

SIGNATURE OVER PRINTED NAME

FOR INTERNAL USE ONLY	
RECEIVED BY:	**REMARKS:**
DATE RECEIVED:	

**** PICs shall only require information that is necessary to the request and to confirm the identity of the requesting individual or his/her authorized representative, taking into consideration the principle of proportionality.***

ANNEX C*

ERASURE REQUEST FORM

(NAME OF PERSONAL INFORMATION CONTROLLER)

I. DATA SUBJECT INFORMATION

FULL NAME	
ADDRESS	
EMAIL ADDRESS	**MOBILE NUMBER**

II. DESCRIPTION OF INFORMATION REQUESTED FOR ERASURE *(Please provide sufficient details about the personal data you are requesting for erasure. Use separate sheet if necessary.)*

III. GROUND/S FOR ERASURE REQUEST *(Mark appropriate boxes as applicable and provide/attach substantial proof.)*

☐ Personal data is: ☐ incomplete ☐ outdated ☐ false or ☐ unlawfully obtained.

Details:

☐ Personal data is used for an unauthorized purpose/s.

Details:

☐ Personal data is no longer necessary for the purpose/s for which they were collected.

Details:

☐ Withdrawal of consent or objection to the processing *(and there are no other applicable lawful criteria for processing).*

Details:

☐ Personal data concerns private information that is prejudicial to data subject

Details:

☐ Processing is unlawful.

Details:

☐ The personal information controller (PIC) or personal information processor (PIP) violated your rights as a data subject.

Details:

IV. DECLARATION

I declare that this form is accomplished by the undersigned and is a true, correct, and complete statement of the information contained herein. I authorize (NAME OF PERSONAL INFORMATION CONTROLLER) to verify/validate the contents stated herein.

SIGNATURE OVER PRINTED NAME

IV. AUTHORIZED REPRESENTATIVES

FULL NAME		
ADDRESS		
EMAIL ADDRESS		**MOBILE NUMBER**

I declare that this form is accomplished by the undersigned as the authorized representative of the data subject. It is a true, correct, and complete statement of the information contained herein. Enclosed is the proof of the authority to act on of behalf of the data subject. I authorize (NAME OF PERSONAL INFORMATION CONTROLLER) to verify/validate the contents stated herein.

SIGNATURE OVER PRINTED NAME

FOR INTERNAL USE ONLY	
RECEIVED BY:	**REMARKS:**
DATE RECEIVED:	

**** PICs shall only require information that is necessary to the request and to confirm the identity of the requesting individual or his/her authorized representative, taking into consideration the principle of proportionality.***