



Administrative Order

No. 19

Series of 2021

**SUBJECT : INTERNAL GUIDELINES ON THE SHARING OF DATA
GENERATED FROM LISTAHANAN**

1. RATIONALE

By virtue of Executive Order No. 867, series of 2010, the DSWD adopted the National Household Targeting System for Poverty Reduction (NHTSPR) or Listahanan. It aims to formulate a unified criteria for the identification of the poor population through scientific means; reduce inclusion/exclusion of beneficiaries of the government's social protection programs through focused targeting; and facilitate sharing of the resulting database to public and private social protection stakeholders.

In carrying out its mandate, the National Household Targeting Office (NHTO), as the lead office in the implementation of the Listahanan project, develops and maintains a database which serves as the repository of data on the poor households. This database is shared and utilized within the Department as well with external stakeholders and partners. As such, provisions to further protect the fundamental human right to privacy of communication while ensuring free flow of information enshrined under R.A. No. 10173 or the "Data Privacy Act of 2012" (DPA) were considered and encapsulated in developing these internal guidelines on data sharing.

The guidelines stated in this Administrative Order (AO) detail the processes involved in the sharing and utilization of Listahanan 3 data to ensure that appropriate procedures are observed in securing data protection and avoid privacy breaches, including unauthorized disclosure of data, whether intended or unintended, within the Department.

2. LEGAL BASES

These guidelines are anchored on the provisions of the following relevant laws and issuances relating to data protection and security, and data sharing.

2.1. Executive Order No. 867, series of 2010

The Order provides for the adoption of the National Household Targeting System for Poverty Reduction as the mechanism for identifying poor households who shall be recipients of social protection programs nationwide. All national government agencies (NGAs) are mandated to use the data generated by the system in prioritizing beneficiaries of the government's social protection programs and projects. Section 2 of the EO

directs the DSWD to maintain the system and serve as the repository of the data on poor households, and update the data every four (4) years.

2.2. Republic Act No. 10173 or the Data Privacy Act of 2012

An Act protecting individual personal information in information and communications systems in the government and private sector. The law protects the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth.

2.3. National Privacy Commission Circular 03 Series of 2020-Section 2F-Data Sharing

The Circular provides the definition of Data Sharing as "the sharing, disclosure, or transfer to a third party of personal data under the custody of a personal information controller to one or more other personal information controller/s.

**2.4. National Privacy Commission Circular 16-01 series of 2016
Security of Personal Data in Government Agencies**

The Circular provides rules to assist government agencies engaged in the processing of personal data to meet their legal obligations under RA No. 10173 and its corresponding implementing rules and regulations. A government agency may use these rules to issue and implement more detailed policies and procedures, which reflect its specific operating requirements.

**2.5. National Privacy Commission Circular 16-02 Data Sharing
Agreements Involving Government Agencies**

Section 1 of the Circular, under General Principle, states that to facilitate the performance of a public function or the provision of a public service, a government agency may share or transfer personal data under its control or custody to a third party through a data sharing agreement; provided, that nothing in the Circular shall be construed as prohibiting or limiting the sharing or transfer of any personal data that is already authorized or required by law.

**2.6. Republic Act No. 6713, Section 7(c). Disclosure and/or misuse of
confidential information**

Section 7(c) of the law stipulates that public officials and employees shall not use or divulge confidential or classified information officially known to them by reason of their office and not made available to the public either (i) to further their private interests or give undue advantage to anyone or (ii) to prejudice the public interest.



2.7. DSWD Memorandum Circular No. 21, series of 2012

Section 4.a of the Enhanced Guidelines on the Code of Conduct for Personnel of the DSWD regardless of the status or manner of engagement states that DSWD personnel shall not disclose any confidential information in the course or by reason of their employment. Confidential information means information that cannot be made public, unless otherwise ordered or authorized by the Court or authorities of the Department, as the unauthorized disclosure thereof may be prejudicial to the interest of the Department, or any of its offices, bureaus, or services or any particular official or employee. This may include, but is not necessarily limited to, the following:

a.1 Sensitive information/data on case studies and personal information of clients

a.1.1 Records of administrative cases involving DSWD personnel

a.2 Notes

a.3 Draft guidelines, memoranda, letters not yet issued or circularized

a.4 Records of deliberations or minutes of meetings not yet finalized, signed, and circulated

a.5 Drafts of concept papers, policy papers, project proposals, etc.

Under Section 4.b of the same MC, DSWD personnel shall not use or divulge confidential or classified information to further their private interests or give undue advantage to anyone or to prejudice public interest.

2.8. National Archives of the Philippines (NAP) General Circular Nos. 1 and 2

The NAP Circulars prescribe the rules and regulations governing the management of public records and set the guidelines on the disposal of valueless records in government agencies.

2.9. Executive Order No. 2, series of 2016

The Order operationalizes in the Executive Branch of government the people's constitutional right to information and the State policies to full public disclosure and transparency in the public service. The EO prescribes the procedures that will guide public officials in ensuring the full protection of an individual's right to information and privacy.

2.10. Republic Act No. 11310 or the Pantawid Pamilyang Pilipino Program Act

Also known as the 4Ps Act prescribes the use of a standardized targeting system to be used in the selection of program beneficiaries, to wit:

Section 5. Selection of Qualified Household-Beneficiaries. On a nationwide basis, the DSWD shall select qualified household-beneficiaries of the 4Ps



using a standardized targeting system. It shall conduct regular revalidation of beneficiary targeting every three (3) years.

Section 6. Eligible Beneficiaries. Farmers, fisherfolks, homeless families, indigenous peoples, those in the informal settler sector, and those in geographically isolated and disadvantaged areas including those in areas without electricity shall be automatically included in the standardized targeting system to be conducted by the DSWD; provided, that to be eligible for the cash grants, households or families must meet the following criteria:

- (a) Classified as poor and near-poor based on the standardized targeting system and the poverty threshold issued by the Philippine Statistics Authority (PSA) at the time of selection;
- (b) Have members who are aged zero (0) to eighteen (18) years old or have members who are pregnant at the time of registration; and
- (c) Willing to comply with the conditions specified by this Act.

2.11. Republic Act No. 11291 or the Magna Carta for the Poor

The law intends to provide an overarching policy in addressing poverty in the Philippines, of which a targeting system and profiling of the poor is important.

Section 7: System for Targeting of Beneficiaries – The NEDA shall maintain and periodically review, in consultation with PSA, a single system of classification to be used for targeting beneficiaries of the government's poverty alleviation program and projects to ensure that such programs/projects reach the intended beneficiaries. The DSWD in coordination with NEDA and the NAPC shall identify the target beneficiaries.

2.12. Republic Act No. 11032 or Ease of Doing Business and Efficient Government Service Delivery Act of 2018 and its Implementing Rules and Regulations

This law aims to promote integrity, accountability, proper management of public affairs and public property as well as to establish effective practices, aimed at efficient turnaround of the delivery of government services and the prevention of graft and corruption in government.

2.13. DSWD Administrative Order No. 20, series of 2019

This Order provides guidance to Department Offices, Bureaus, Service, and Field Offices in streamlining the process of delivery of DSWD's services, in compliance with relevant laws, rules and regulations.

2.14. DSWD Memorandum Circular No. 8, series of 2020

The document details the simplified data sharing guidelines on the provision of DSWD programs and services during a national state of emergency.



2.15. Memorandum Circular No. 12 series of 2017 Guidelines in sharing the data generated from the Listahanan 2

The guidelines establish a systematic way of sharing data as well as information on poor households that may be eligible for various social protection programs and services; ensuring that mechanisms to safeguard the personal and sensitive personal information of households in the Listahanan database are in place.

2.16. Administrative Order 008 series of 2017 Guidelines in Accessing the Result of Listahanan 2 for DSWD Field Offices

This guidelines facilitates sharing of the results of Listahanan 2 specifically with DSWD Offices. It will strengthen the mechanism for data sharing by ensuring compliance to pertinent laws including Republic Act 10173 otherwise known as the Data Privacy Act of 2012 and Executive Order No. 02, Series of 2016 on the Freedom of Information.

2.17. DSWD Special Order (SO) No. 2323, series of 2020

The SO designates Personal Information Controllers (PIC), Data Protection Officers (DPO), and Compliance Officers for Privacy (COP). In addition to the designation of PIC, DPO, and COP for each DSWD OBSUs both at the Central and Field Offices, the SO also specified the functions, roles, and responsibilities of each position.

3. DEFINITION OF TERMS

- 3.1. Anonymizing** refers to the stripping or disguising of an information that could be used to identify an individual from a data set. It is used to prevent identification of the individual either directly or by deduction.
- 3.2. Compliance Officer for Privacy (COP)** is an individual or individuals who ensures that all office procedures conform to the data privacy protocols.
- 3.3. Data Center** refers to a centralized repository, which may be physical or virtual, may be analog or digital, used for the storage, management, and dissemination of data including personal data.
- 3.4. Data Generation** refers to the phase covering the data mining activity and the preparation of requested data on the poor in electronic form. All data requests generated involving personal and sensitive personal information shall be prepared in electronic form that is encrypted and password-protected.
- 3.5. Data Protection Officers (DPO)** are individuals designated by the Personal Information Controller and tasked to ensure compliance with applicable laws and regulations for the protection of data privacy and security. DPOs shall manage the privacy aspect in the different areas of operations and who shall plan, implement, and evaluate policies for data privacy and security.



Under the National Privacy Commission (NPC) Advisory No. 2017-01 or the Designation of Data Protection Officers (DPO), the DPO "shall be accountable for ensuring the compliance by the PIC or PIP with the DPA, its IRR, issuances by the NPC, and other applicable laws and regulations relating to privacy and data protection."

For government agencies and instrumentalities, designated DPOs must be an organic employee of the agency (NPC Circular 16-01 Section 3, F).

- 3.6. **Data Sharing** is the disclosure or transfer of information and/or personal data to another party under the custody of a personal information controller or personal information processor.
- 3.7. **Data Sharing Agreement** refers to a contract, joint issuance, or any similar document that contains the terms and conditions of a data sharing arrangement between two or more parties: Provided, that only personal information controllers (PIC) shall be made parties to a data sharing agreement.
- 3.8. **Name-Matching** is an activity undertaken primarily to determine if a household is in the Listahanan database with corresponding poverty status.
- 3.9. **Near Poor** households are those with estimated per capita income 10% above the poverty threshold, but are at high risk of subsequently falling into poverty.
- 3.10. **Personal data** is any information relating to an individual that identifies the individual or can be used to identify them. A person can be identified directly from data such as their name, surname, and identification number, etc. They may be identified indirectly from data that describes recognizable attributes, such as specific physical, physiological (including biometric and genetic), behavioral, mental, economic, cultural, or social characteristics. International data protection laws typically distinguish between categories of personal data, depending on how strictly the information must be protected. These categories are defined as follows:

Personal Information refers to information whether recorded in material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

Sensitive Personal Information refers to personal information about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations. It also includes information on an individual's health, education, genetic or sexual life, or to any proceedings for any offense committed / alleged to have been committed by such person, the disposal of such proceedings or the sentence of court proceedings. If lost, compromised, or disclosed without authorization, this could result in



substantial harm, embarrassment, inconvenience, or unfairness to an individual.


- 3.11. **Personal data breach** refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.
- 3.12. **Personal Information Controller (PIC)** is 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.
- 3.13. **Personal Information Processor (PIP)** refers to any natural or juridical person qualified to act as such to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.
- 3.14. **Processing** refers to any operation 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.
- 3.15. **Raw Data** are data commonly referred to as source data which are unprocessed anonymized data that can be transformed into different formats. These data are usually used for research.
- 3.16. **Statistics** are numerical processed data that are formatted in tabular and graphical form that can be used for analysis, inferences, and other interpretations.

4. OBJECTIVES

Data generated from the Listahanan shall be shared primarily to serve as basis in prioritizing beneficiaries of social protection programs as mandated by EO No. 867. These guidelines specifically aim at:

- 4.1. Establishing a systematic way of sharing data as well as information on poor households that may be eligible for various anti-poverty programs and services;
- 4.2. Ensuring that mechanisms to safeguard or protect the personal and sensitive personal information of households in the Listahanan are in place; and
- 4.3. Increasing coordination on the use of data generated from the Listahanan vis-à-vis other databases of households utilized by the DSWD OBSUs in the development and implementation of social protection programs and services.

5. COVERAGE



These guidelines shall apply to all DSWD Offices, Bureaus, Services, Units (OBSUs) at the Central and Field Offices, as well as Centers, Residential Care Facility, Sections, and Units (CRCFU) at the regional level and attached agencies.

6. GENERAL GUIDELINES

- 6.1.** All requests for Listahanan data must undergo a process that includes the review of the request as to purpose and kind of data needed, and securing approval of authorized officials for data generation of such to ensure that the personal data, statistics, and raw data requested will indeed be used for social protection programs or activities such as, but not limited to, provision of social services or enrolment in poverty reduction programs, academic advancement (dissertation, thesis, term papers, etcetera), research, and program or project development.

The request must contain information necessary for the sharing of personal data including the specific data requirements, data format (i.e. Excel, CSV, SQL), processes to be applied to the personal data, and the list of names of the staff and respective position titles who will be authorized to access Listahanan data, and which shall form part of the details of the transfer.

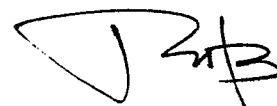
- 6.2.** All Memorandum of Agreement (MOA)/Non-Disclosure Agreement (NDA) on the access to previous Listahanan databases are deemed revoked upon availability of the updated official Listahanan results. Sharing of the latest Listahanan data involving personal and sensitive personal information of the poor shall be facilitated upon the execution and compliance to the procedures provided in this Order.

- 6.3.** The NHTO reserves the right to approve or disapprove any request for data or information, upon conduct of an assessment whether the disclosure of such information or data will violate existing laws or any Department policies.

An appeal to review the merits of a disapproved request must be made in writing to the NHTO Head / Regional Director within seven (7) working days upon receipt of the notice of denial of request for data. A response shall be given within seven (7) working days from the date of receipt of the review request.

- 6.4.** The formula of the Proxy Means Test (PMT) used in identifying the poor households is strictly confidential and shall not be shared with any stakeholder, regardless of its purpose.

- 6.5.** The questionnaire or the Household Assessment Form (HAF) used to collect household information, whether hard or electronic copy, may be shared with the requesting party. The administration of the form, however, shall be the exclusive responsibility of the NHTO and its regional components, the National Household Targeting Section (NHTS).



- 6.6. The Listahanan Operations Manual and Field Workers Manuals may be shared with the requesting party, upon approval of a written request indicating the purpose.
- 6.7. For any written document/report and IEC materials such as audio-visual presentations produced out of Listahanan data, proper credit or citation to the DSWD Listahanan as the source of data shall be made. These materials shall also be shared with the DSWD.
- 6.8. OBSUs are not permitted to share the Listahanan database containing personal information (PI) and sensitive personal information (SPI) to third parties external to the Department. Requests for such should be solely referred to the NHTO or NHTS as may be the case.

7. DATA PROTECTION AND SECURITY

Consistent with Rules VI and VII of the Data Privacy Act, the designated data users or personal information controllers (PIC) shall establish organizational, physical, and technical security measures for data protection. These measures shall maintain the integrity and confidentiality of personal data, and prevent negligent, unlawful, or fraudulent processing, access, disclosure, and destruction of personal data.

To facilitate the release of requested data and ensure compliance with applicable laws and regulations for data protection and security, all OBSUs and attached agencies will be required to comply with the following:

- 7.1. Designate at least one (1) DPO within the office/agency who shall plan, implement, and evaluate policies for data privacy and security as well as be authorized to review and respond to information requests and complaints concerning the processing of personal data. The office/agency can also designate a COP, as long as the COP shall be under the supervision of the DPO.
- 7.2. Put in place appropriate physical, technical, and organizational measures to protect the personal data generated from the Listahanan database against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access, as well as other unlawful processing.
 - a. Physical and technical requirements¹ shall include: (1) a secured, dedicated, and monitored workstation or data center having an operating system (OS) with antivirus and antimalware software, and MySQL version 5.7 or higher, where the Listahanan data will be stored; and (2) a secured and monitored network such as, but not limited to, a server farm and firewall.

¹ The NHTO reserves the right to determine the appropriate requirements for each type of data format, i.e. Excel, CSV, and SQL.



- b. Organizational requirements include: (1) designation of a DPO duly registered with the National Privacy Commission (NPC); (2) certification or designation of the list of identified personnel who will access, process, and safeguard the data; and (3) procedures or protocols so any person or party authorized to access the personal data will be legally answerable to the Second Party.
- 7.3.** Establish required procedures or protocols so that any person or party acting under the authority of the end-user with access to the personal data will be answerable administratively and legally to respect and maintain the confidentiality and security of the personal data, and shall be obliged to process the personal data only per instructions; and
- 7.4.** Inform the NHTO DPO in writing, within seventy two (72) hours upon knowledge of, in cases of data breaches which includes unauthorized acquisition of the data subjects' PI, SPI, or other information that, under the circumstances, may be used to enable identity fraud or give rise to a real risk of serious harm to the data subjects.

The designated DPO of the OBSU shall respond to information requests from data subjects, using NPC Circular No. 2021-01 as reference, and complaints concerning processing of the personal data, and will coordinate in good faith with the NHTO, the data subject, and the National Privacy Commission concerning all such inquiries within a reasonable time.

The requesting OBSU must have the capacity to organize appropriate teams to respond to and handle incidences of data and security breach. At the Central Office, the organization of these response teams are under the purview of the Data Protection Officer.

8. DATA SHARING PROCEDURES

The NHTO shall, at all times, adhere to the principle of proportionality in the sharing of Listahanan data, whereby 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 be reasonably fulfilled by other means.

8.1. National-level Request for Personal Information

- a. For requests involving personal and sensitive personal information of data subjects, the following are the requirements:
 - i. Letter of Request addressed duly signed by the Head of Office (HOO) and addressed to the NHTO Director indicating purpose for the request, the list of data sets required and how these will be used, and a reasonable timeline as to when the requested data is needed;
 - ii. Document indicating the appointed and NPC-registered Data Protection Officer;



- iii. Accomplished Non-Disclosure Agreement² signed by the HOO as Personal Information Controller (PIC) and designated DPO/COP upon approval of the request;
 - iv. List of personnel who will have access to the Listahanan data together with the purpose and data processing they will employ in the treatment of data; and
 - v. Signed Certificate of Acceptance³.
- b. The designated DPO shall review the request and make recommendations to the NHTO Director.
 - c. If approved, the NHTO Director shall forward the request to the NHTO Information Technology Division for data generation. If denied, the NHTO shall prepare a Denial of Request for Data Form highlighting the grounds for such denial. This shall be communicated within seven (7) working days upon receipt of the request.
 - d. The NHTO shall release to the authorized personnel of the requesting office the compact disk, USB stick, or hard drive containing the encrypted and password-protected Listahanan data as well as the password to access the data in the disk or drive.

8.2. Regional-level Request for Personal Information

- a. For requests involving personal and sensitive personal information of data subjects, the following are the requirements:
 - i. Letter of Request addressed to the Policy and Plans Division (PPD) Chief indicating purpose, specific data sets needed, and a reasonable timeline for the expected release of the data, signed by the Regional Project Coordinator (RPC), Regional Field Coordinator (RFC) or Division Chief;
 - ii. Document indicating the appointed and NPC-registered Data Protection Officer;
 - iii. Accomplished Non-Disclosure Agreement signed by the HOO as PIC and designated DPO/COP upon approval of the request;
 - iv. List of personnel who will have access to the Listahanan data together with the purpose and data processing they will employ in the treatment of data; and
 - v. Signed Certificate of Acceptance upon receipt of the requested data.
- b. The designated DPO shall review the request and make recommendations to the Regional Director.
- c. If approved, the Regional Director shall forward the request to the NHTS for data generation. If denied, the NHTS shall prepare a Denial of Request for Data Form highlighting the grounds for such denial. This

² See Annex A

³ See Annex B

shall be communicated within seven (7) working days upon receipt of the request.

- d. The NHTS shall release to the authorized personnel of the requesting office the compact disk, USB stick, or hard drive containing the encrypted and password-protected Listahanan data as well as the password to access the data in the disk or drive.

8.3. To facilitate name-matching, the requesting office shall prepare a Letter of Request indicating the reasons for name-matching and enclosing an electronic copy⁴ of the names of households to be matched. The e-file must include the following minimum fields⁵:

- Complete name (last name, first name, middle name, extension name)
- Birthdate (YYYY-MM-DD)
- Address (province, city/municipality, and barangay information)
- Philippine Standard Geographic Code (PSGC) province, city/municipality, and barangay

Upon approval, the requesting office shall also submit an accomplished Non-Disclosure Agreement signed by the HOO as PIC and the designated DPO/COP to the NHTO or NHTS.

After the appropriate data requisition and clearance, the timeframe for the processing of name-matching requests is as follows:

Number of Records	Duration
Less than 5,000	1 working day
5,001 to 50,000	5 working days
50,001 to 400,000	15 working days
More than 400,000	30 working days

Depending on the number of records requested for matching, the results shall be shared as attachment to an official response memorandum or through a password-protected shared drive link.

To guarantee data privacy and security, name matching shall only be done at the Central Office through the NHTO Information Technology Division and at the DSWD Field Offices (FOs) through the NHTS using the name matching application.

⁴ In MS Excel/CSV format

⁵ One field per column



- 8.4. For statistical and anonymized data, the requesting party must submit a Letter of Request signed by the HOO or the RPC, RFC, or Division Chief, and addressed to the NHTO Director (for national/multi-region statistics) or PPD Chief (for regional-level statistics) indicating the required data sets, purpose of the request, and a reasonable timeline for the expected release of the data.

8.5. Data Sharing During National Emergency

While the sharing of data in times of national emergency is inevitable, this must still be regulated in accordance with existing laws and policies. Section 12 of the Data Privacy Act provides for the criteria for lawful processing of personal information. One of these relates to the mandate of public authorities, i.e., when processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate. It shall follow the principle of proportionality wherein the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to the declared and specified purpose. Further, personal data shall be processed only if the purpose of the processing could not be reasonably fulfilled by other means.

Requests for data during a national emergency must be supported with the following:

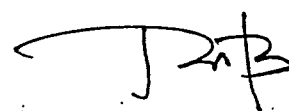
- a. A letter of request, duly signed by the HOO, indicating the purpose and use of the data being requested, and the government declaration or resolution on the state of emergency defining the scope, coverage, and timeframe;
- b. Accomplished non-disclosure agreement covering the duration of the state of emergency; and
- c. Name of authorized personnel who shall receive the data and other personnel who will have access to the data.

9. FEEDBACK REPORTING

All users of Listahanan data are required to submit a utilization report using the prescribed template⁶ on how the data was utilized in the development and implementation of specific programs and services for the poor. For one-time programs/projects with a fixed duration period, an interim report must be submitted to the NHTO or NHTS three (3) months after initial program/project implementation and another upon conclusion of the program/project. For recurring programs, an annual utilization report must be submitted to the NHTO or NHTS six (6) months after initial implementation and every year thereafter.

10. RETENTION AND RECORDS DISPOSAL

⁶ See Annex C



The retention and disposal of Listahanan records shall be governed by pertinent provisions of NAP Circulars 1 and 2. The NHTO supports the principle that all records should be managed in a way that allows the information contained within them to be available to the person who needs them, at the time and place where they are needed.

11. PENALTIES

Penalties shall be imposed for data breaches committed by officials and employees as prescribed under Chapter VIII, Sections 25 to 37 of the Data Privacy Act.

Upon the declaration of a competent court that data privacy rights were violated, the Department may terminate its Data Sharing Agreement and demand the deletion of the data from the end user's database, without prejudice to the filing of the appropriate legal action.

12. EFFECTIVITY

This Administrative Order takes effect immediately and revokes all previous issuances contrary thereto.

Issued in Quezon City this 22nd day of October 2021.


ROLANDO JOSELITO D. BAUTISTA
Secretary

Cert. True Copy:

MYRNA H. REYES
OIC-Division Chief
Records and Archives Mgt. Division
26 OCT 2021

CONFIDENTIALITY AGREEMENT

KNOWN ALL MEN BY THESE PRESENTS:

This Agreement made and entered into and between:

The Department Of Social Welfare And Development (DSWD) with office address at Batasang Pambansa Complex, Constitution Hills, Quezon City, herein represented by **Andrew J. Ambubuyog, Director IV, Concurrent Head of the National Household Targeting Office**, hereinafter referred to as the "First Party";

- and -

The following **DSWD Field Office** personnel of legal age from the [requesting office], herein referred to as the "Second Party":

NAME

POSITION

ADDRESS

- WITNESSETH -

1. The First Party provides the Second Party privileged access to Listahanan database, applications, systems and other equipment that contain the records and information of the households which are private and confidential in nature.
2. The Second Party has privileged access to Listahanan database, applications, systems, and other equipment that contain records and information of the households which are private and confidential in nature. The Second Party, as the **DESIGNATION OF STAFF/S WHO WILL PROCESS/ACCESS THE DATA**, is entrusted with the privileged access and encounter to sensitive, confidential or proprietary information whether or not it is labelled or identified as such. It is mutually understood that all household assessment forms accomplished and received by the Second party, related to the Listahanan is a property of the First Party.
3. The Second Party agrees that he/she will only use and access information available to him/her in the course of his/her duties, and not to engage in any activity that conflicts with the interest of the First Party, nor convey, sell or use any access to information available to him/her, and to provide information to others engaged in any activity that conflicts the interest of the First Party. With respect to Listahanan's Household Assessment Form (HAF), system, network, records, files, electronic mail and other information, the Second Party agrees that he/she will treat all as confidential information,

and as such, respects the privacy of users, and the integrity of the systems, and other related physical resources, and he/she will:

- a. Access, copy, or store data solely in performance of his official responsibilities, limiting perusal of contents and actions taken to the least necessary to accomplish the task;
 - b. Copy or store data or information only with the First Party's consent and only to complete a specified task, and only to copy and store user data enough to complete the specified task;
 - c. Not seek personal benefit or permit others to benefit personally from any data or information that has come to him/her through work assignments;
 - d. Not make or permit authorized use of any information of the First Party's information systems or records;
 - e. Not enter, change, delete or add data to any information system or file outside of the scope of his/her responsibilities;
 - f. Not intentionally or knowingly, or cause to be included in any form, record or report, a false, inaccurate or misleading entry;
 - g. Not intentionally or knowingly alter or delete, or cause to be altered or deleted from any forms, records, report or information system, a true and correct entry;
 - h. Not intentionally or knowingly alter, change, delete or add codes to any information system or similar systems deployed in the any servers of the DSWD;
 - i. Not release First Party's data other than what is required for the completion of his/her job responsibilities;
 - j. Not exhibit or divulge the contents of any record, file or information system to any person except as required for the completion of his/her job responsibilities;
 - k. Take every reasonable precautions to prevent unauthorized access to forms, password, user identification, or other information that is used to access the First Party's information system or records;
 - l. Limit access to information contained in or obtained from the systems to authorized persons; and
 - m. Be prohibited to use and access personal USB, electronic mail and social networking sites while in the performance of his official responsibilities.
4. The Parties involved may withdraw from this Agreement only if the Second Party surrenders to the First Party all credentials, documents, information, and data received for the activity.
 5. The Second Party understands and agrees that breach of confidential information shall be subjected to court litigation in accordance with Section 28, 29, 31, 32, and 33 of Republic Act No. 10173 or the "Data Privacy Act of 2012".

Annex A: Template for Non-Disclosure Agreement

6. The Second Party understands and agrees that failure to comply with the terms of this agreement will have consequences and may result in disciplinary action up to immediate termination of his/her engagement with criminal prosecution, depending upon the severity of infraction, evidence of the intentions, and the sensitivity and scope of the information compromised.
7. The Second Party agrees to the foregoing terms and conditions and that the Agreement remains in effect continuously until termination of the engagement. He/she further agrees that, upon termination of engagement with the First Party, he/she will not keep in his/her possession, recreate or deliver to anyone else, any confidential, sensitive, or proprietary information, whether or not is labelled as such, acquired while he/she is engaged with the First Party.

IN WITNESS WHEREOF, We have hereto signed this Agreement on this ____day of ____,
2021 in _____, Philippines.

[NAME]
Regional Director
DSWD Field Office []

[NAME]
[Position]
[Office/Bureau/Section]
[Agency Name]

Signed in the presence of:

[NAME]
[Division Chief/COP]
Policy and Plans Division/NHTS
[DSWD Field Office]

[NAME]
[Division Chief/COP]
[Requesting Office]
[DSWD Field Office]

ACKNOWLEDGEMENT
REPUBLIC OF THE PHILIPPINES
() S.S.

BEFORE ME, a Notary Public, for and in the above jurisdiction, personally appeared the following:

NAME	COMPETENT EVIDENCE OF IDENTITY	DATE/PLACED ISSUED
Andrew J. Ambubuyog	_____	_____
[Name/s of second party]	_____	_____

Known to me to be the named persons who executed the foregoing instrument and they acknowledged to me that the same is their own free will and voluntary act and need.

This instrument consists of four (4) pages including this page wherein this Acknowledgement is written, and is signed by the parties and their instrumental witnesses on each and every page hereof.

WITNESS **MY** **HAND** **AND** **SEAL**, this _____ day of _____, 20____ at _____, Philippines.

NOTARY PUBLIC

Doc No. _____;
Page No. _____;
Book No. _____;
Series of 20 _____.

LISTAHANAN DATA UTILIZATION REPORT

I. ORGANIZATIONAL INFORMATION

Name:	
Address:	
Head of Organization:	
Nature of Organization:	
Vision	
Mission	
Objectives	

II. SOCIAL PROTECTION DESCRIPTION

- a. Project/program and services
(Please describe the programs and services your organization provided to the households indicated in the Listahanan database)
- b. Project/program beneficiaries
(Please describe how many and how the aforementioned programs and services assisted the households indicated in the Listahanan data that we shared)
- c. Enumerate the materials prepared or developed such as reports, IEC material which the Listahanan 3 Data shared with you served as reference
- d. Coverage
(Specify the areas/geographical location where the program is implemented)

III. ISSUES/PROBLEMS ENCOUNTERED

	CHALLENGES	ACTIONS TAKEN	NEXT STEPS
1			
2			

TRANSFORMATION/PROCESSING UNDERTAKEN

(Specify if there are transformation/other processing undertaken on the Listahanan 3 database/result)