OFFICE OF THE VICE PRESIDENT
THE REPUBLIC OF INDONESIA

Indonesia's Unified Database for Social Protection Programmes

Management Standards

TNP2K
NATIONAL TEAM
FOR THE ACCELERATION OF POVERTY REDUCTION

Indonesia’s Unified Database for Social Protection Programmes

TNP2K
NATIONAL TEAM
FOR THE ACCELERATION OF POVERTY REDUCTION

Indonesia's Unified Database for Social Protection Programmes

Management Standards

INDONESIA'S UNIFIED DATABASE FOR SOCIAL PROTECTION PROGRAMMES – MANAGEMENT STANDARDS

July 2015

Cover Photo: Joshua Esty

To request a copy of this report or further information, please contact the TNP2K Knowledge Management Unit (kmu@tnp2k.go.id).

This report is also available at the TNP2K website (www.tnp2k.go.id).

NATIONAL TEAM FOR THE ACCELERATION OF POVERTY REDUCTION

Secretariat of the Vice President of the Republic of Indonesia
Jl. Kebon Sirih No. 14 Central Jakarta 10110
Telephone: (021) 3912812 | Facsimile: (021) 3912511
E-mail: info@tnp2k.go.id
Website: www.tnp2k.go.id

Contents

List of Figures

List of Tables

List of Photos

List of acronyms and abbreviations

ANSI/TIA	American National Standards Institute/ Telecommunications Industry Association
Bappenas	National Development Planning Board *(Badan Perencanaan dan Pembangunan Nasional)*
BLSM	Temporary Unconditional Cash Transfers *(Bantuan Langsung Sementara Masyarakat)*
BLT	Unconditional Cash Transfers programme *(Bantuan Langsung Tunai)*
BPS	Statistics Indonesia *(Badan Pusat Statistik)*
BSM	Cash Transfers for Poor Students programme *(Bantuan Siswa Miskin)*
CCTV	closed-circuit television
CD	compact disc
CPU	central processing unit
DPM	beneficiaries list *(Daftar Penerima Manfaat)*
FLOOD	a type of denial of service attack on a computer system
Genset	backup electrical generator
ICT	information and communication technology
ISO/IEC JTC	International Organisation for Standardisation and the International Electrotechnical Commission Joint Technical Committee
ISP	internet service provider
Jalinkesra	Alternatives for Social Welfare *(Jalan Lain Menuju Kesejahteraan)*
Jamkesmas	Public Health Insurance programme *(Jaminan Kesehatan Masyarakat)*
JPS	Social Safety Net programme *(Program Jaring Pengaman Sosial)*
JPS-BK	Social Safety Net Health Agency programme *(Program Jaring Pengaman Sosial Badan Kesehatan)*
KPS	Social Protection Card *(Kartu Perlindungan Sosial)*
KUR	Credit for Businesses programme *(Kredit Usaha Rakyat)*
LAN	local area network
OPK	Special Markets Operation – later Raskin *(operasi pasar khusus)*
P4S	Programme for Expanding and Accelerating Social Protection *(Program Perluasan dan Percepatan Perlindungan Sosial)*
PKH	Conditional Cash Transfer Programme for Families *(Program Keluarga Harapan)*
PNPM	National Programme for Community Empowerment *(Program Nasional Pemberdayaan Masyarakat)*
Podes	survey of villages *(Potensi Desa)*
PPLS	Data Collection for Social Protection Programmes carried out by Statistics Indonesia in 2011.

PSE	: Socioeconomic Data Collection *(Pendataan Sosial Ekonomi)*
RAID 5	: a system of backup drives for extra security
RAM	: random access memory
Raskin	: Rice for the Poor (*(Program Subsidi Beras bagi Masyarakat Berpendapatan Rendah)*
Raskinda	: Locally implemented Raskin programme *(Raskin Daerah)*
RTHM	: near poor households *(rumah tangga hampir miskin)*
RTM	: poor households *(rumah tangga miskin)*
RTSM	: very poor households *(rumah tangga sangat miskin)*
Sejahtera	: Prosperous
Susenas	: National Socioeconomic Survey *(Survei Sosial Ekonomi Nasional)*
TKPK	: coordination teams for poverty reduction *(Tim Koordinasi Penanggulangan Kemiskinan)*
TNP2K	: National Team for the Acceleration of Poverty Reduction *(Tim Nasional Percepatan Penanggulangan Kemiskinan)*
UDB	: Unified Database for Social Protection Programmes *(Basis Data Terpadu untuk Program Penanggulangan Kemiskinan – BDT)*
UPS	: uninterrupted power supply
UPSPK	: National Targeting Unit *(Unit Penetapan Sasaran Untuk Penanggulangan Kemiskinan)*
VPN	: virtual private network

Foreword

The Unified Database (UDB) contains the names, addresses and socioeconomic data for approximately 24.7 million Indonesian households – some 96.4 million of Indonesia's poorest – and plays a significant role in efforts to improve the targeting of beneficiaries of poverty reduction programmes.

The UDB's data is managed by the National Targeting Unit for Poverty Reduction (UPSPK), within the Secretariat of the National Team for the Acceleration of Poverty Reduction (TNP2K). The UPSPK's main role is to ensure that the UDB can be accessed and used by social protection programmes, provide technical support to UDB users, monitor and evaluate how the UDB is used, ensure the validity of studies aimed at improving programme targeting, improve the use of information technology in the management of the UDB, and deliver the information contained in the UDB via the internet.

Managing such a large amounts of data and meeting high-standards of accountability requires staff who have special skills and competencies, as well as appropriate data management standards to ensure that the data is utilized effectively. The book, "Indonesia's Unified Database - Management Standards", looks at the lessons learned from managing a large volume of data as well as provides guidelines on how the management of the database should be done in the future.

We would like to express our gratitude to the team of writers who have helped produce this book. We hope it will benefit all those who are committed to and understand the importance of data management in reducing poverty in Indonesia.

Jakarta, July 2015

Dr. Bambang Widianto
Deputy to the Vice President, Human Development and Equitable Development Policy Support and Executive Secretary for the National Team for the Acceleration of Poverty Reduction.

1

Background

BACKGROUND

Reducing poverty and improving community well-being are key goals in Indonesia's Medium-term National Development Plan Phase II (2010–2014). With the target of reducing national poverty levels from 14.1 percent in 2009 to 8–10 percent by the end of 2014, the government, through Presidential Regulation no. 15 of 2010, developed a strategy and established a programme to achieve this goal. The government programmes designed to accelerate poverty reduction consist of three main components:

1. Individual, family or household based programmes, grouped into cluster 1, aim to provide basic rights, lessen life's burdens and improve the quality of life for the poor. Cluster 1 includes rice subsidies for low-income households, the Rice for the Poor programme (referred to as the Raskin programme), the Cash Transfers for Poor Students programme (*Bantuan Siswa Miskin* – BSM), the public health insurance programme (referred to as Jamkesmas) and the Conditional Cash Transfer Programme for Poor Families (*Program Keluarga Harapan* – PKH).

2. Programmes based on community empowerment are grouped into cluster 2. These programmes aim to develop and strengthen the capacity of poor communities to get involved in development, based on the principles of community empowerment. Cluster 2 includes the National Programme for Community Empowerment (known as PNPM) which operates at both urban and rural levels.

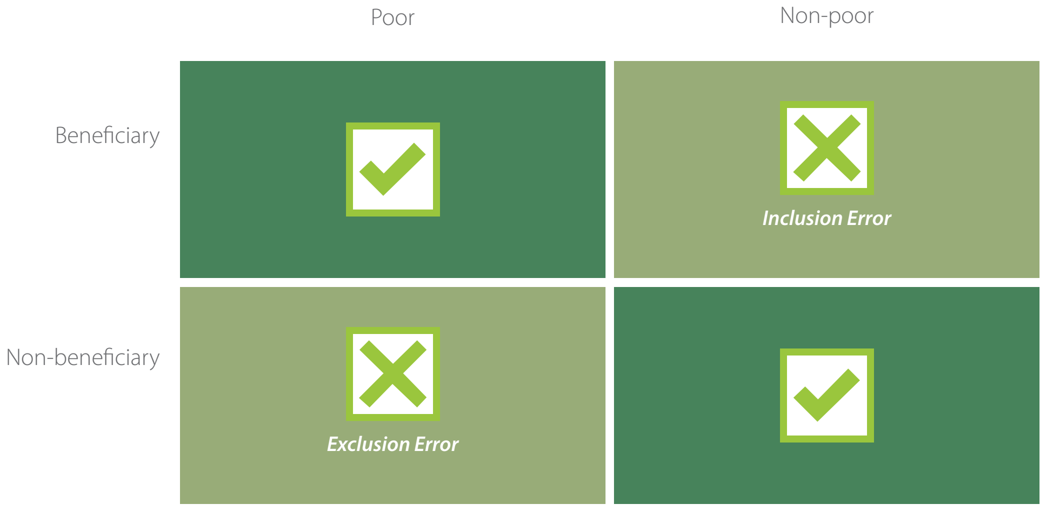
3. Programmes based on empowering micro and small businesses are grouped into cluster 3. These programmes aim to improve people's access to the economy and to strengthen micro and small-scale trade. One initiative in cluster 3 is the Credit for Businesses programme (*Kredit Usaha Rakyat* – KUR).

In addition to these programmes, other activities have been initiated to reduce poverty rates, increase economic activity and promote the well-being of low-income groups.

With the Presidential Regulation no. 15 of 2010 as its cornerstone, the government set up the National Team for the Acceleration of Poverty Reduction (*Tim Nasional Percepatan Penanggulangan Kemiskinan* – TNP2K). TNP2K is chaired by the Vice President of Indonesia and is tasked with developing policies and programmes to synergise poverty reduction activities across various ministries and agencies, as well as with overseeing and controlling programme implementation. At the provincial and regency or city levels, mandates were granted to establish coordination teams for poverty reduction (TKPK). These are chaired by the regional deputy heads and coordinate poverty reduction in their respective districts while also overseeing poverty reduction policies and programmes under the direction of the national team.

One of the priorities on TNP2K's agenda in the short to medium term is to unify the national targeting system. This mechanism is used to identify individuals, families and households entitled to some form of protection or assistance (social security) from central and local governments (Widianto 2012). A targeting system is considered effective if it can reduce both exclusion and inclusion errors among beneficiaries participating in a programme (Figure 1).

Figure 1. Schematic representation of inclusion and exclusion errors in targeting beneficiaries of social protection programmes

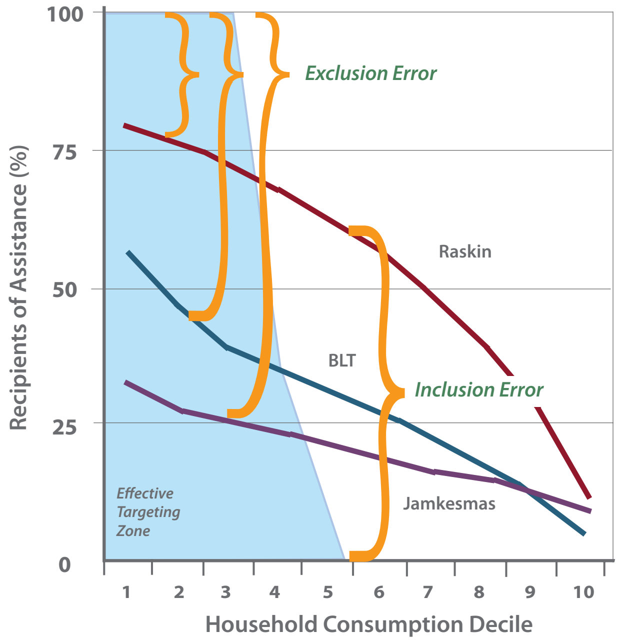


	Poor	Non-poor
Beneficiary	✓	✗ *Inclusion Error*
Non-beneficiary	✗ *Exclusion Error*	✓

Source: TNP2K

Since 1998, the Indonesian government has implemented a number of social protection programmes targeting the poor, including Raskin, Jamkesmas, the Unconditional Cash Transfers programme (*Bantuan Langsung Tunai* – BLT) and others. An analysis of data from the National Socioeconomic Survey (known as Susenas) in 2009 showed high inclusion and exclusion error rates in the targeting of these programmes (Figure 2). The 2009 survey also indicated that only about 30 percent of the poor received benefits from all three social protection programmes implemented by the government at that time, namely Raskin, Jamkesmas and the BLT programme.

Figure 2. Effectiveness of social welfare programmes



Source: Susenas 2009

One reason for the inefficient targeting of these programmes was that programme operators used different databases to identify potential participants. Experience from many countries[1] shows that having a UDB that can be used to identify participants or beneficiaries for many different programmes can significantly improve the effectiveness of social protection programmes.

THE EVOLUTION OF TARGETING SYSTEMS DEPLOYED FOR SOCIAL PROTECTION PROGRAMMES IN INDONESIA

Prior to 1998, there were no specific social protection policies in Indonesia. At that time the government applied macro strategies such as stabilising food prices, developing rural infrastructure and implementing a few credit programmes to reduce poverty.

Following the Asian financial crisis of 1997–1998, the government began to design and implement programmes specifically targeting the poor. To counter the impact of the financial crisis, the government launched the Social Safety Net programme (*Program Jaring Pengaman Sosial* – JPS) which aimed to assist with food security, health, education

[1] **Example:** Ficha de Estratificacion Social Comite Accion Social (Ficha CAS) in Chile, and Sistema de Identificacion de Beneficiarios de Subsidios Sociales (Sisben) in Colombia.

and access to income for residents who were poor prior to or as a result of the crisis. The JPS activities that had the largest number of targeted participants were the rice subsidy programme for poor households (initially called Special Markets Operation or OPK and later changed to Raskin) and the social safety net health agency programme (*Program Jaring Pengaman Sosial Badan Kesehatan* – JPS-BK). To target participants both these programmes used geographical approaches to identify areas where potential participants lived and to determine if they met the criteria specified in the programme's objectives (Sumarto, Suryahadi and Widyanti 2002).

Targeted participants of the OPK/Raskin and JPS-BK programmes were classified as either "pre-prosperous" (*prasejahtera*) or "prosperous 1" (*sejahtera 1*) families[2], as determined by the criteria of the National Family Planning Coordinating Board. The board prepared a list of targeted households based on data they collected using 23 variables as indicators of a household's welfare status (TNP2K 2015).

Some studies on the coverage of the rice subsidy and social safety net programmes suggest that exclusion and inclusion error rates were high. A 1997–1998 study involving 100 villages or subvillages in ten regencies in eight Indonesian provinces reported that the proportion of the poorest households participating in the rice subsidy programme was only 52.7 percent while about 20 percent of households in the highest quintile group also received subsidised rice. As for JPS-BK, only about 10.6 percent of the poorest group received health care benefits (Sumarto, Suryahadi and Widyanti 2002). The use of non-economic indicators (for example, the ability to fulfill religious obligations) by the National Family Planning Coordinating Board as criteria for determining a household's welfare status, as well as the lack of qualified cadres to collect the data, were among several factors that prevented the data from correctly targeting beneficiaries.

[2] **Pre-prosperous (pra-sejahtera) families** are unable to fulfill their basic needs for education, clothing, food, health care and their religious obligations. Prosperous 1 (sejahtera 1) families can fulfill their basic needs but have not been able to provide for the family's psychological and social needs, such as education for all family members, family planning, and effectively participating in the community (provided by the translator from: https://statistikaterapan.files.wordpress.com/2011/02/pengertian-keluarga-sejahtera.pdf)

In 2005, the government, through Statistics Indonesia (*Badan Pusat Statistik* – BPS), carried out a survey known as the Socioeconomic Data Collection (*Pendataan Sosial Ekonomi 2005* – PSE 2005). The main objective of this data was to identify households entitled to the Unconditional Cash Transfers as compensation for the reduction in fuel subsidies. But in addition to this programme, the PSE 2005 data was also used to target potential beneficiaries of the Health Insurance for the Poor programme (originally known as Askeskin) and also to assist with the Raskin programme. The health insurance programme for the poor later became the Public Health Insurance programme and is currently known as Jamkesmas.

The PSE 2005 identified 14 non-monetary variables to use in measuring the well-being of households (Table 1). Each of these variables was weighted and then recorded in a household welfare index. Based on the welfare index, 19.1 million households were recorded in the 2005 PSE as very poor (*Rumah Tangga Sangat Miskin* - RTSM), poor (*Rumah Tangga Miskin* – RTM) or almost poor (*Rumah Tangga Hampir Miskin* - RTHM).

The PSE 2005 approach to classifying household welfare status using 14 variables was considered less sensitive than the National Family Planning Coordinating Board method, as discussed in a report by the National Development Planning Board (Bappenas 2010) that evaluated family planning services for the poor in 2010. The report pointed out that the quota that Jamkesmas used, based on the estimated number of poor people in the PSE 2005, was smaller than in the National Family Planning Coordinating Board classification, so that most families classified as "pre-prosperous" and "prosperous 1" were not eligible for free access to family planning services in health centres, clinics and hospitals.

Table 1. Variables in the Socioeconomic Data Collection 2005 (PSE 2005)

Variables in household prosperity	Criteria for being classified as poor
1. The area of floor space per household or family member	< 8m^2
2. The type of floor in the house	Earth/plywood/low quality
3. The type of walls in the house	Bamboo, poor quality plywood
4. Toilet facilities	Not present
5. Availability of drinking water	Clean water unavailable
6. Type of lighting used	Not electric
7. Fuel used	Wood/charcoal
8. Number of meals per day	Less than two
9. Ability to buy chicken, meat or milk every week	No
10. Ability to buy new clothes for each household member	No
11. Ability to get treatment at a local community clinic	No
12. Household head's type of work or job	Small-scale farming, fishing, gardening
13. Household head's level of education	Never attended school/Did not complete year six
14. Ownership of assets / valuables worth at least Rp500,000	None

Source: SMERU 2006

In 2008, as part of the framework to distribute the Unconditional Cash Transfers programme, Statistics Indonesia provided socioeconomic data on targeted households[3] which was then called the Data Collection for Social Protection Programmes (*Pendataan Program Perlindungan Sosial 2008*, popularly known as PPLS 2008).

The basic data for the PPLS 2008 came from PSE 2005 data that had been updated with verified information from 1,023 subdistricts in 97 regencies or cities in 15 provinces that carried out trials for the Conditional Cash Transfer Programme for Poor Families (PKH), which brought the final number of targeted households to 19,018,057 (Imawan 2008). Ranking the welfare status of households was based on PPLS 2008 data which still used the very poor, poor or almost poor classification system. However, PPLS 2008 added eight extra individual household variables to the 14 used in PSE 2005 and deployed proxy means testing models to rank improvements in the welfare status of the households assessed (Ritonga 2014).

In addition to being used for targeting in the Unconditional Cash Transfers programme, household micro data from PPLS 2008 was used to set the goals for the Conditional Cash Transfer Programme for Poor Families (PKH) from 2009 to 2011. It was also used to identify especially poor households entitled to other forms of assistance to improve their welfare, such as Jalinkesra, a poverty reduction initiative implemented by the provincial government of East Java between 2010 and 2013.

DEVELOPING THE UNIFIED DATABASE (UDB)

The Unified Database for Social Protection Programmes (hereafter the UDB) was set up using data from the updated Data Collection for Social Protection Programmes carried out by Statistics Indonesia in 2011. This survey is known as PPLS 2011. It took advantage of the momentum from the 2010 census which comprehensively updated Indonesia's national population data. The 2010 census provided the baseline data used to identify households to be included in PPLS 2011.

A number of improvements were made in the methodology applied to collect and process the data, including:

1. The earlier lists of households, compiled through poverty mapping, were complemented with the results of consultations with low-income groups and through impromptu discussions and general observations;

[3] Presidential Instruction RI No. 3 of 2008.

2. More variables were used to measure the well-being levels of households, compared with the PPLS 2008 (26 as opposed to 14); and
3. The coverage of households was greater than it was for the PPLS 2008 , reaching 40 percent of the population or approximately 24 million households.

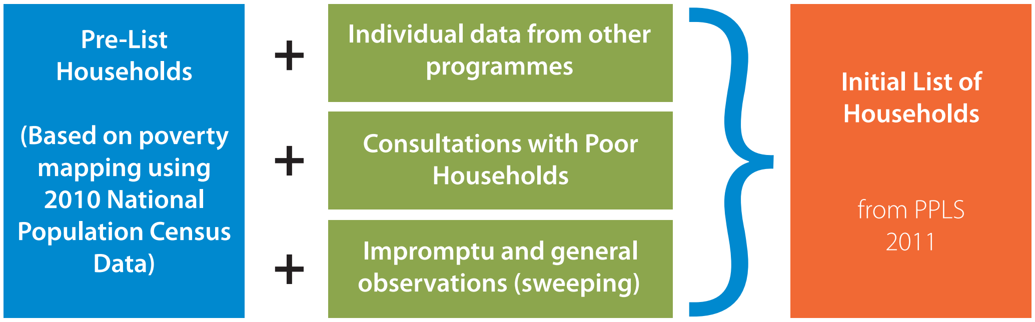
Table 2. Variables in the Data Collection for Social Protection Programmes, 2011 (PPLS 2011)

Individual variable	Household variable
Name	Owns a home
Age	Measurement of floor area
Gender	Primary type of flooring in the house
Marital status	Primary type of walls in the house
Relationship with the household's head and family	Primary type of roof on the house
In possession of an identity card	Availability of clean drinking water
Disabilities	Procedure for obtaining clean drinking water
Chronic illnesses	Main source of lighting
Pregnancy status	Main type of fuel used for cooking
School attendance	Owns a toilet
Level of education	Assets owned
Duration of schooling	Participates in the family planning and cluster 1 programmes
Currently employed	
Type of job or work	
Work status	

Source: PPLS 2011

Statistics Indonesia conducted the PPLS 2011 between July and October 2011. As illustrated in Figure 3, the initial list of households was obtained through poverty mapping using data from the 2010 population census, the 2010 socioeconomic survey (Susenas) and Podes which is village-level data compiled by Statistics Indonesia. In addition to households already identified, the PPLS 2011 officers identified other potentially poor households through consultations with members of other poor households, impromptu conversations and general observations during the process of collecting data. All households recorded during this process were included in the initial PPLS 2011 list of households.

Figure 3. The procedure for obtaining the initial list of households – PPLS 2011


Pre-List Households

(Based on poverty mapping using 2010 National Population Census Data)

+ Individual data from other programmes

+ Consultations with Poor Households

+ Impromptu and general observations (sweeping)

Initial List of Households

from PPLS 2011

Source: TNP2K

Statistics Indonesia submitted the PPLS 2011 data to TNP2K in February 2012. The welfare status of each household was indexed using the variables in household welfare obtained during PPLS 2011 and using proxy means testing models. The models used to process the PPLS 2011 household data included references to the 2010 National Socioeconomic Survey (Susenas) in order to provide a statistical picture of household characteristics and to accommodate differences in characteristics between regions. TNP2K developed proxy means testing models specific to each regency and city since a variable affecting household welfare status in one city or regency may have little significance somewhere else. For example, in rural areas, owning a motorcycle may be a distinguishing variable in determining a household's welfare status but this would probably not be the case in most urban areas.

Based on the well-being index generated by the proxy means testing models, household data from PPLS 2011 was sorted from lowest to highest according to welfare status. The information processed from PPLS 2011 provided the source data to develop a Unified Database for Indonesia's social protection programmes that came into effect in March 2012.

INFORMATION IN THE UDB

The database contains socioeconomic and demographic information for approximately 40 percent of the population with the lowest welfare status. This amounts to about 24 million households or around 96 million individuals. In each area, the number of people included in the database varies according to the region's poverty levels. Provinces, regencies and cities with lower levels of poverty will have fewer households in the UDB.

The Unified Database classifies households into deciles. Deciles divide households into 10 groups, as follows:

- Decile 1 refers to the 10 percent of households who are the poorest – with the lowest levels of well-being;
- Decile 2 refers households that are within the 10–20 percent poorest; and so on, up to
- Decile 10 which covers households in the top 10 percent in terms of wealth or with the highest level of well-being.

The UDB contains deciles 1, 2, 3 and 4 because it includes the 40 percent of households that are economically the least well-off in Indonesia. The database can provide data about the distribution or aggregation of individuals, families and households according to socioeconomic variables recorded in the PPLS 2011, as well as socioeconomic details and names and addresses of those registered in the UDB.

TNP2K AS OVERSEER OF THE UDB

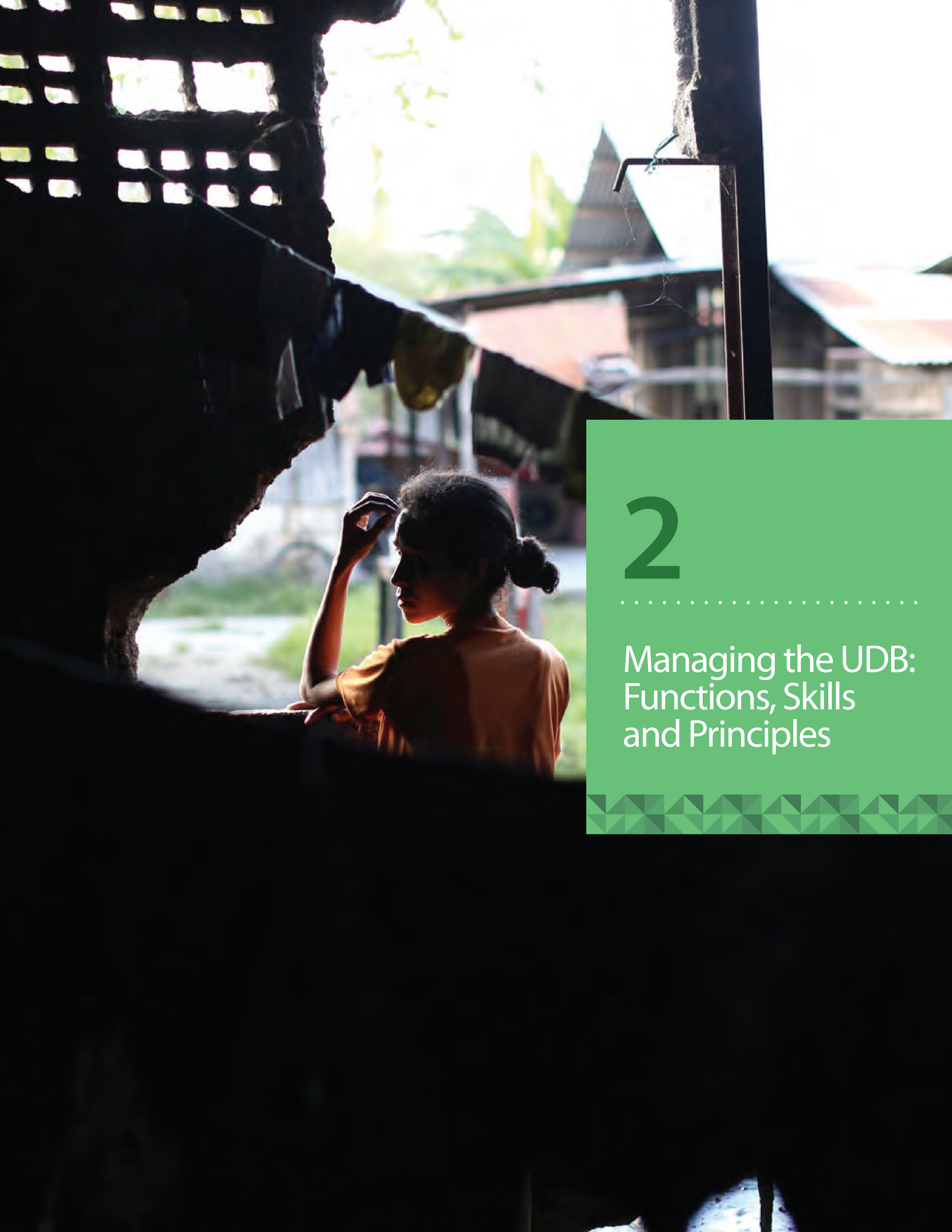
The National Targeting Unit (*Unit Penetapan Sasaran Untuk Penanggulangan Kemiskinan* – UPSPK) was set up to enable TNP2K to fulfil its role in formulating policies and programmes to synergise poverty alleviation activities in other ministries and agencies. It is managed by the secretariat of TNP2K.

The brief for UPSPK[4] includes:

- Facilitating the use of the UDB for social protection programmes by providing technical support to users;
- Evaluating usage of the database;
- Ensuring the validity of studies undertaken to improve targeting in the database;
- Developing strategies to manage the database; and
- Making information in it publicly available using internet-based technologies.

[4] **Decree No. 9 of 2012** by the Deputy Secretary for the Vice President for People's Welfare and Poverty in his role as the Executive Secretary for TNP2K..

Since the inception of the UDB in March 2012, UPSPK has handled more than 700 requests for data and more than 1,000 requests for technical support. The database has been used to define and set goals for the Raskin, PKH, BSM and Jamkesmas programmes. It was also used to determine which households should receive social protection cards (*Kartu Perlindungan Sosia*l – KPS) which were launched in conjunction with the Temporary Unconditional Cash Transfer initiative (*Bantuan Langsung Sementara Masyarakat* – BLSM) and the Programme for Expanding and Accelerating Social Protection (*Program Perluasan dan Percepatan Perlindungan Sosial* – P4S). By June 2014, approximately 60 percent of provincial, regency and city level governments had accessed the UDB for use in planning and implementing their own locally-funded social assistance programmes. TNP2K staff and researchers from other institutions have also used the database for poverty-related research (for example, Lockley et al. 2013).



2

Managing the UDB: Functions, Skills and Principles

MANAGING THE UDB: FUNCTIONS, SKILLS AND PRINCIPLES

The main role of the management unit is to oversee the access to and use of the database by stakeholders involved in social protection programmes. In line with these objectives, the management unit has three main functions:

1. **To use appropriate technology to organise and manage the data system**
   The management unit is responsible for building systems for the database; identifying and installing compatible software to operate it; formulating and implementing information and communication technology (ICT) policies and protocols to ensure the availability, security and integrity of the data; and providing access to the variety of information that is potentially available from the database through information technology based media.

2. **To provide operational data services**
   The management unit's aim in providing operational services is to ensure that the UDB is used in the research, planning, implementation, monitoring and evaluation of poverty reduction and social assistance programmes. Accordingly, it is responsible for providing data and technical support to users and for promoting a unified national targeting system so that the UDB becomes the primary data source for identifying target beneficiaries of social assistance programmes. The management unit also promotes awareness of the importance of the UDB among stakeholders at the national and regional levels, and fosters cooperation with users and other UDB stakeholders to encourage data sharing and to monitor how UDB data is used.

3. **To develop knowledge related to targeting social protection programmes**
   The management function includes activities to build and evaluate the methodology and procedures for identifying households to be targeted by social protection programmes and recommending ways to improve the national targeting system. It provides statistical analyses from the UDB and other poverty-related reports to help improve the design and management of social assistance initiatives, as well as regular updates to enhance the accuracy and integrity of the data.

To support these various functions, unit managers need to:

1. Be able to design and articulate policies that support planning and budgeting for poverty reduction and social protection programmes implemented by the government.

2. Be academically qualified at the postgraduate (Sarjana 2) level or have relevant and verifiable skills and knowledge in the field of information management systems and technology, including statistics, economic development, social welfare, public administration, social security, demographics, public communication, management, political science and social interventions; and

3. Be experienced in planning, implementing, monitoring and evaluating social protection programmes, especially in the areas of health, education, food, finance (conditional and unconditional cash transfers), economic accessibility and increased access to infrastructure.

In carrying out its functions and applying the relevant laws and regulations, the management unit needs to adhere to the following work principles:

- **Ensure the UDB is inclusive**
  The management unit must facilitate access to and use of UDB data by both government and non-government agencies in accordance with its stated purpose and without charge.

- **Respect the integrity of citizens' personal data**
  The Central Information Commission Decision no. 187 / V / KIP.PS.MA / 2012, ratified during the Open General Assembly on 18 March 2013, stated that UDB data is exempt from the rules of Act No. 14 of 2008 on Public Information because it meets the criteria specified in article 17h concerning personal data:

  - The history and status of family members;
  - The health history, ailments, treatment, medication, physical health and psychological status of individuals;
  - An individual's financial status, assets, income and bank account details;
  - Personal information concerning the individual's formal or non-formal education.

In accordance with article 15, paragraph 1 of Government Regulation no. 82 of 2012 on Implementing an Electronic Transaction Management System, the management unit must ensure that all data concerning an individual's name and address remains confidential and that the acquisition and use of names and addresses of individuals is with the consent of the owner of the private data at the time of the PPLS 2011 when data was collected to implement government programmes.

Data containing names and addresses of individuals in the UDB are only issued to government agencies (central and local) that organise social assistance programmes. Government agencies that access data containing the names and addresses of individuals in the UDB must take responsibility for maintaining the integrity and confidentiality of the individual data, as set forth in the Memorandum of Cooperation Agreement (for the ministries and ministry-level agencies) and the Letter of Declaration (for local government agencies).

- **Be accountable**

  In accordance with articles 9, 10, 11 and 12 of Act no. 14 of 2008 on Public Information and article 11 paragraph 1 of Commission Regulation no. 1 of 2010 concerning Public Information Services Standards, the the UDB management unit must periodically provide a summary report on access to the UDB that includes at least:

  - The number of requests to access UDB data received;
  - The time taken to respond to requests asking to access the data;
  - The number of requests for UDB data that were granted, either partially or completely, as well as the number of requests that were denied; and
  - The reasons for denying requests for UDB data.

In carrying out these duties, the management unit is responsible for: openly developing the procedures for accessing and using the UDB; making this information publicly available; and implementing a consistently-applied data access request system including supporting documentation and technical support.

3

Managing requests for UDB Data and Technical Support

MANAGING REQUESTS FOR UDB DATA AND TECHNICAL SUPPORT

In principle, UDB data can be used by a variety of institutions involved in social protection programmes and/or poverty reduction efforts, including government agencies (central and regional), academic and research institutions, agencies cooperating across ministries, and government and non-government institutions. The UDB management unit is responsible for ensuring that any access to UDB data is in accordance with the duties and authorities of the institutions requesting the data and that no data published is changed by users who lack the requisite authority.

ACCESSING AND USING THE UDB

The main benefits of the UDB for social protection programmes are in planning, analysing and determining target beneficiaries, and in monitoring and evaluating programme implementation. The UDB management unit can provide data in different ways, depending on the intended purpose and it can be distributed as aggregated data, or individual data with or without names and addresses (Table 3).

Table 3. Summary of the UDB data profile

No	Reason for Access	Aggregated Data	Individual data without names and addresses	Individual data with names and addresses
1.	Planning/Analysis of Social Protection programmes	V	V	
2.	Target beneficiaries, social protection programmes monitoring and evaluation			V

Source: TNP2K

Using the UDB to plan and analyse social protection programmes

Aggregated data, as well as individual data without names and addresses from the UDB can be used to perform various analyses of the poor, design poverty reduction programmes and estimate a programme's budgetary requirements. These data are provided for various agencies involved in planning, implementing and monitoring social protection programmes, including government agencies, research institutions and non-governmental organisations.

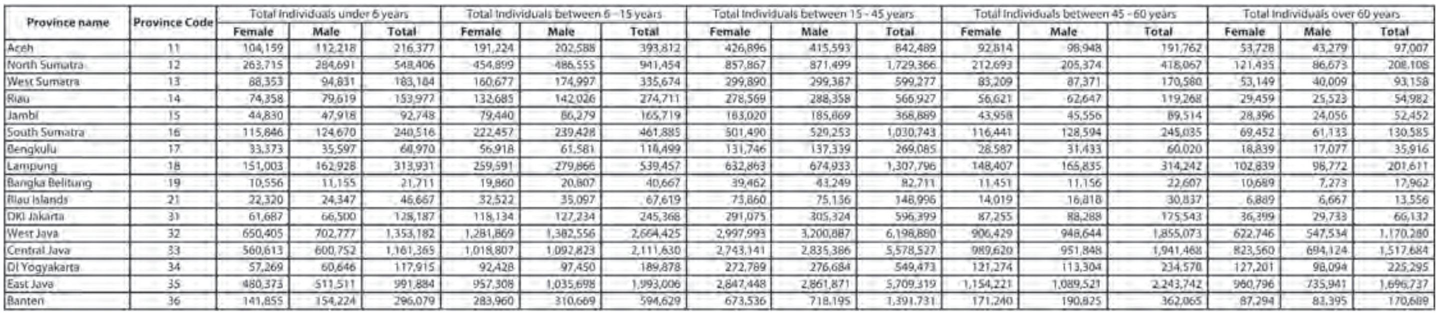
The UDB's aggregated data can provide information about the total number of individuals, families and households, based on the variables recorded in the PPLS 2011, for example:

- The number of families with school-aged children (7-18 years);

- The total number of school-aged children (7-18 years) attending or not attending school; and
- The number of households that do not yet have decent sanitary facilities.

In accordance with the needs of the applicant requesting data from the UDB, aggregated data can be provided for the provincial level through to the village and village subdistrict levels. Table 4 shows an example of aggregated data from the UDB.

Table 4. Example of distributed/aggregated data from the UDB



Province name	Province Code	Total Individuals under 6 years			Total Individuals between 6 - 15 years			Total Individuals between 15 - 45 years			Total Individuals between 45 - 60 years			Total Individuals over 60 years		
		Female	Male	Total	Female	Male	Total	Female	Male	Total	Female	Male	Total	Female	Male	Total
Aceh	11	104,159	112,218	216,377	191,224	202,588	393,812	426,896	415,593	842,489	92,814	98,948	191,762	53,728	43,279	97,007
North Sumatra	12	263,715	284,691	548,406	454,899	486,555	941,454	857,867	871,499	1,729,366	212,693	205,374	418,067	121,435	86,673	208,108
West Sumatra	13	88,353	94,831	183,184	160,677	174,997	335,674	299,890	299,387	599,277	83,209	87,371	170,580	53,149	40,009	93,158
Riau	14	74,358	79,619	153,977	132,685	142,026	274,711	278,569	288,358	566,927	56,621	62,647	119,268	29,459	25,523	54,982
Jambi	15	44,830	47,918	92,748	79,440	86,279	165,719	183,020	185,869	368,889	43,958	45,556	89,514	28,396	24,056	52,452
South Sumatra	16	115,846	124,670	240,516	222,457	239,428	461,885	501,490	529,253	1,030,743	116,441	128,594	245,035	69,452	61,133	130,585
Bengkulu	17	33,373	35,597	68,970	56,918	61,581	118,499	131,746	137,339	269,085	28,587	31,433	60,020	18,839	17,077	35,916
Lampung	18	151,003	162,928	313,931	259,591	279,866	539,457	632,863	674,933	1,307,796	148,407	165,835	314,242	102,839	98,772	201,611
Bangka Belitung	19	10,556	11,155	21,711	19,860	20,807	40,667	39,462	43,249	82,711	11,451	11,156	22,607	10,689	7,273	17,962
Riau Islands	21	22,320	24,347	46,667	32,522	35,097	67,619	73,860	75,136	148,996	14,019	16,818	30,837	6,889	6,667	13,556
DKI Jakarta	31	61,687	66,500	128,187	118,134	127,234	245,368	291,075	305,324	596,399	87,255	88,288	175,543	36,399	29,733	66,132
West Java	32	650,405	702,777	1,353,182	1,281,869	1,382,556	2,664,425	2,997,993	3,200,887	6,198,880	906,429	948,644	1,855,073	622,746	547,534	1,170,280
Central Java	33	560,613	600,752	1,161,365	1,018,807	1,092,823	2,111,630	2,743,141	2,835,386	5,578,527	989,620	951,848	1,941,468	823,560	694,124	1,517,684
DI Yogyakarta	34	57,269	60,646	117,915	92,428	97,450	189,878	272,789	276,684	549,473	121,274	113,304	234,578	127,201	98,094	225,295
East Java	35	480,373	511,511	991,884	957,308	1,035,698	1,993,006	2,847,448	2,861,871	5,709,319	1,154,221	1,089,521	2,243,742	960,796	735,941	1,696,737
Banten	36	141,855	154,224	296,079	283,960	310,669	594,629	673,536	718,195	1,391,731	171,240	190,825	362,065	87,294	83,395	170,689

Source: UDB July 2012

Data without names and addresses provides information about the characteristics of individuals, families or households (for example, age, gender, employment, housing conditions, education) but without the names or addresses of the individuals, families or households concerned. This data can be used to analyse the characteristics of poverty or evaluate the effectiveness of programme targeting.

Using the UDB to determine target beneficiaries and to monitor and evaluate social protection programme implementation

The UDB can provide **data with the names and addresses** of the individuals, families or households. This can be used to identify those who meet the criteria to become programme participants or beneficiaries, as determined by programme organisers. This data is given to government offices (ministry-level government agencies and local governments) that manage social protection programmes, at both central and regional levels.

An example of this type of UDB data is the beneficiary list for the Raskin programme. Since 2012, the UDB has been used to determine the target households or individual beneficiaries for a number of social protection programmes, such as central government programmes (for example, the Raskin programme in 2013 and 2014, the Jamkesmas

programme in 2013, the PKH and the BSM programmes) and those managed by local governments (for example, the regional health insurance programme (Jamkesda) and the locally funded Raskin programme (Raskinda). To help determine social protection programme beneficiaries, the UDB published a list of individuals, families and households that were potentially eligible. For example, in 2013, the Coordinating Minister for People's Welfare, as chairperson of the Raskin coordinating team, stipulated that 15.5 million of Indonesia's poorest households would be target beneficiaries of the Raskin programme.

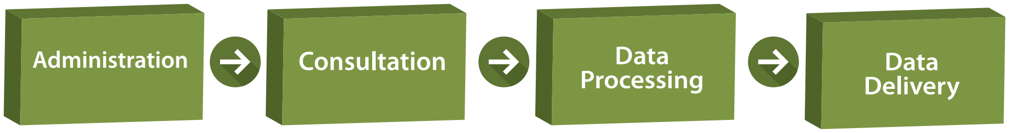
Based on this criteria, the UDB identified households and published a list containing the names and addresses of the heads of each household. The list, known as "Beneficiaries list 1" (DPM 1), was handed over in a public ceremony to the minister in his role as chairperson of the Raskin coordinating team. Another example of using the UDB to target beneficiaries was for Jamkesmas, the public health insurance programme, in 2013. The Ministry of Health, which oversaw Jamkesmas decided that the programme would target 86.4 million of Indonesia's poorest individuals. Accordingly, the UDB published a list of 86.4 million names and addresses of the poorest individuals. This amounted to around 21 million households. Unlike the Beneficiaries list 1, which included only the names and addresses of the heads of households, the Jamkesmas list included the names and addresses of each individual beneficiary. Thus, the two lists of beneficiaries may look as though they come from different databases.

Once the UDB has provided the information, each social protection programme implementer is responsible for distributing, verifying, updating and using the list of the beneficiary names and addresses. The process of distributing, verifying, updating and using the UDB target data of beneficiaries is described in more detail in chapter 5.

PROVIDING UDB SERVICES

Data from the UDB is provided at **no cost** and within 15 working days of the request. The process of handling requests for data consists of four phases, as illustrated in Figure 4.

Figure 4. The stages in handling UDB requests



Source: TNP2K

Stage 1 : Administration

Under Government Regulation no. 82 of 2012 on the Implementation of Electronic Systems and Electronic Transactions, people managing electronic data must be prepared to report on the data they manage. In effect, this means that every request for UDB information must be made in writing to the management unit and the release of the information must be similarly recorded. The documentation is to ensure there is a record of the origin, number and types of requests for UDB information received and the data provided. Nevertheless, distributed or aggregated data can be provided via the Internet because the information delivered by this means protects the privacy of the individuals, families and households in the UDB. The management unit can choose only the most commonly used variables for planning social protection programmes to put online and make publicly available. These include:

- The status of household and individual well-being;
- Female heads of households by age;
- The welfare status of individuals by age and gender;
- Children attending or not attending school, by age;
- Individuals attending school by gender and type of school attended;
- Toilet facilities;
- Landfills for disposal of fecal waste;
- Disabilities by age and gender;
- Chronic diseases by age and gender;
- Individuals employed or not employed by age;
- The head of household's type of work;
- The type of work performed by individuals aged 18-60 years;
- Residential status;
- Source of drinking water;
- Primary source of lighting; and
- Type of fuel used for cooking.

The level and depth of information provided is determined by the purpose of the request and the sensitivity of the data involved, as summarised in Table 5. A request for data can be made by a formal letter to the management unit that explains the purpose of the data, the variables required, the distribution or aggregation required and the geographical coverage (for example, the province, regency, city). For the purposes of research or analysis, the UDB can provide data without individual names and addresses that can be accessed by many parties, including government agencies, academic institutions, civil society organisations and students working on dissertations related to social protection programmes. Applications for the purposes of research are made through a formal letter to the management unit explaining the nature of the research. Individual researchers, for example, students working on dissertations or theses, need official clearance from their institutions to confirm their identity and student or employee status.

Central and regional government agencies that deliver social protection programmes can access the individual data from the UDB that includes names and addresses if it is to determine programme beneficiaries. Ministries or agencies at central government level that deliver social protection programmes can apply for a list of names and addresses from the UDB by submitting a formal letter to the management unit explaining the selection criteria and the number of programme beneficiaries. Ministry and agency unit managers and the management unit then prepare a Joint Memorandum of Understanding on the use of the UDB, as shown in annex 1.

Local governments that require individual data containing names and addresses to determine programme targets or beneficiaries can request this in a formal letter to the management unit that includes:

- A description of the programme and the criteria for determining the target beneficiaries (see annex 2); and
- An affidavit confirming their responsibility to protect the integrity of the 'Individual' data containing names and addresses stored in the UDB (using the format shown in annex 3).

Table 5. Supporting documentation for UDB requests

			Supporting Documentation		
No	**Intended use of the data**	**Type of data**	**Ministry/Agency (central government)**	**District level government)**	**Other agencies or individuals**
1.	Programme planning or analysis	Aggregated data	Data request letter		
2.	Programme research, monitoring or evaluation	Individuals' data **without** names and addresses	- Data request letter - Research paper		
		Individuals' data **with** names and addresses	- Information about the programme to be monitored and/or evaluated		
			- Data request letter - Memorandum of Understanding (annex 1)	- Data request letter - Information about the programme (annex 2) - Affidavit confirming responsibility for protecting the data's integrity (annex 3)	Invalid because the applicant making the request is not a provider of social protection programmes
3.	Determining the programme's targets/beneficiaries	Individual's data **with** names and address			

Source: TNP2K

Stage 2: Consultation

After the administrative details of the data request have been provided, the management unit contacts the officials appointed by the applicant agencies or institutions to clarify the details of the requested data, including the variables and format of the data required, and to establish whether the UDB can fulfill the request and how it will be delivered to the applicant.

Stage 3: Data processing

The management unit accesses and processes the UDB data according to the requirements of the applicant confirmed during consultations. After the data has been processed, it is checked to ensure it is complete before being copied on to a compact disc (CD).

Stage 4: Data delivery

A CD containing the data is delivered to the applicant by post or in person if the applicant is able to come in to the UDB management unit's office. The designated officer from the management unit contacts the agencies or institutions concerned to notify them that the data they requested can be collected or delivered.

UDB TECHNICAL SUPPORT SERVICES

Technical assistance in using the UDB aims to promote its benefits and potential applications, as well as ensure that the data provided can be used by the requesting parties. The management unit provides technical assistance before, during and after the actual data is requested. Other technical assistance includes, for example, discussions and consultations, public awareness activities, training and matching other data to work with the UDB.

Consultations regarding the database are available to applicants requiring technical assistance through visits to the UDB office or by requesting information on the phone or via email. Management unit representatives assist with applicants' technical needs as far as possible. Ministries or agencies, local governments, academic institutions and other institutions, as well as the public, can consult the management unit.

Applicants seeking technical assistance or activities to promote awareness about the UDB can write a letter to the head of the management unit. A representative will visit the applicant's location and act as a resource person on using UDB data. In general, technical assistance is provided to ministries or agencies, local governments, universities, donors and civil society organisations.

UDB training comprises special technical assistance for local governments seeking help in planning an assistance programme. Local governments can request technical assistance by writing a formal letter to the head of the management unit. Assistance is provided over two days in the form of documentation, presentations and group work The information presented during the training includes, for example: the reasons for establishing the UDB; how it was developed; the difference between Susenas and the UDB; accessing and using the UDB; as well as other topics reflecting the need to constantly change the database to support the accuracy, verification, validation and updating of the data.

Other forms of technical assistance include configuring data independently developed by ministries and agencies so that it is compatible with the UDB. Examples of compatibility activities conducted with other institutions include synchronising data such as post codes or population identity numbers or developing a local database.

HANDLING REQUESTS FOR DATA AND TECHNICAL ASSISTANCE

This section outlines the different stages in handling requests for data and technical assistance. Generally, the head of the management unit applies a time frame of 15 days for completing such requests, starting the day all the necessary documentation is received.

Process for handling requests for data

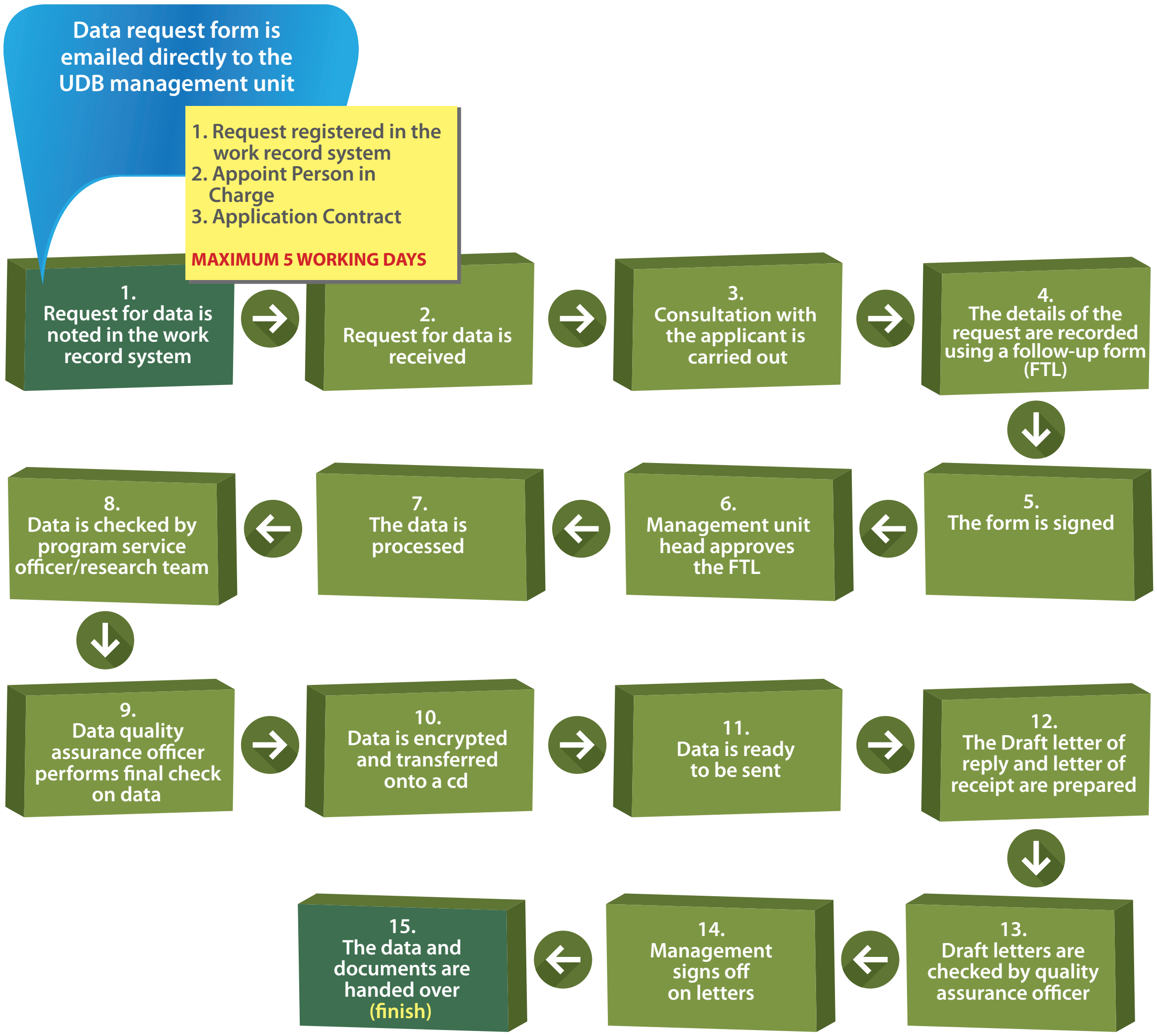
An overview of the process the management unit uses to handle requests for data is shown in figure 5, while descriptions of the tasks involved are shown in table 6. Approved requests for data are recorded in the work record system. The management unit officer assigned to handle the request, as the authorised person in charge, delegates the required follow-up action from a member of the work group.

The delegate contacts the applicant to arrange a consultation. The consultation usually considers matters such as the criteria for the data required by the social assistance programme and the completeness of their existing data. Next, a follow-up form from the system's record of work is printed out and initialled by the data quality assurance officer (operations coodinator) and a request for approval is submitted to the unit manager. Then the extracted data is reviewed by the delegate and the research team before being returned to the data quality assurance officer for a further review to ensure its accuracy. If adjustments are required, the prepared data has to be returned to the data extractor.

The management unit delegate then drafts a reply and a letter of receipt. At this point the status of the data is referred to as "data ready to be delivered". After that, the draft reply and letter of receipt are reviewed by the data quality assurance officer and then sent to the unit head for initialling.

Finally, the letter of reply is forwarded to the management unit head for signature. The data is either posted to the applicant or collected personally. If the data has been sent, the applicant must return a letter of receipt via email or fax to the management unit head and the password for the data is provided. If the data is collected personally, the password can be given to the applicant immediately after the receipt is signed.

Figure 5. Handling requests for data


Data request form is emailed directly to the UDB management unit
1. Request registered in the work record system
2. Appoint Person in Charge
3. Application Contract
MAXIMUM 5 WORKING DAYS
1. Request for data is noted in the work record system
2. Request for data is received
3. Consultation with the applicant is carried out
4. The details of the request are recorded using a follow-up form (FTL)
5. The form is signed
6. Management unit head approves the FTL
7. The data is processed
8. Data is checked by program service officer/research team
9. Data quality assurance officer performs final check on data
10. Data is encrypted and transferred onto a cd
11. Data is ready to be sent
12. The Draft letter of reply and letter of receipt are prepared
13. Draft letters are checked by quality assurance officer
14. Management signs off on letters
15. The data and documents are handed over (finish)

Source: TNP2K

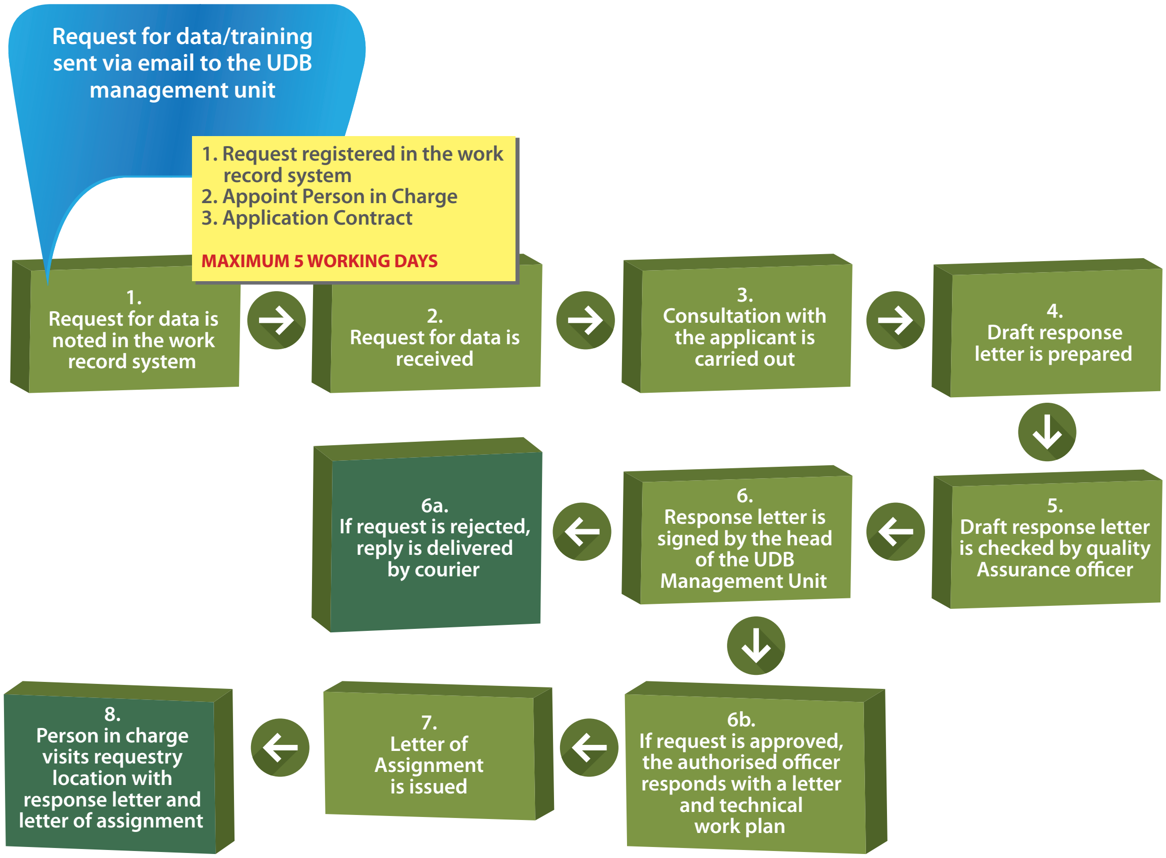
Table 6. Details of the process for handling requests for data

Numbered stages	Stage	Process details
1-2	**Request for data is received**	a. The applicant's documentation is checked in accordance with the type of request submitted. b. The documents supporting the request for data are presented to the UDB management unit Head for approval and follow-up
1-2	**Request for data is noted in the work record system.**	Applications approved for follow-up are listed in the work record system.
2	**Responsibility for handling the request is assigned to an authorised officer.**	The unit head or officer responsible delegates the follow-up action for handling the data request to a member of the authorised work group.
3	**Consultation with the applicant is carried out.**	The delegate contacts the applicant or representative in order to: - Reconfirm the request for data - Determine the details and level of data requested - Explain the process involved and the time required until the data can be sent / handed over.
4	**The details of the request are recorded using a follow-up form (FTL)**	a. The delegate records the outcome of the consultation with the applicant in an electronic follow-up form in the work record system. b. The follow-up form is printed and delivered to the management unit head Unit Pengelola BDT
5-6	**The follow-up form is reviewed and a decision reached**	a. The management unit head reviews the follow-up form and makes any needed revisions. b. The form is signed and sent to the data processing officer.
7	**The data is processed**	(Explained in chapter 4)
8-9	**The data is printed**	The data quality assurance officer (PMD) does a final check on the accuracy of the data.
10-14	**Electronic copies of the data and supporting documents are prepared**	a. The data is encrypted in an electronic file b. The encrypted data is copied on to a compact disk (CD) c. The CD is labelled according to the number and name of the registered application as lodged in the work record system. d. The CD, a letter of reply and a letter of receipt are sealed in an envelope bearing the UDB logo.
15	**The data and documents**	a. The envelope containing the CD, letter of reply and a letter of receipt is sent to the applicant or his delegate b. The management unit gets confirmation from the contracted courier service that the package has been delivered c. The delegated officer from the management unit confirms with the applicant that the package was received and asks for a completed letter of receipt to be sent d. After receiving the fully completed letter of receipt, the password for the data is provided e. The officer records the letter of receipt in the work record system and closes the request.

Process for handling requests for technical help

When requests for technical assistance are received, the designated delegate contacts the person or organisation making the request and discusses their technical needs. The usual procedure for handling such requests is shown in Figure 6 and details of the tasks involved are shown in table 7.

Figure 6. The process for handling requests for technical assistance


Request for data/training sent via email to the UDB management unit
1. Request registered in the work record system
2. Appoint Person in Charge
3. Application Contract
MAXIMUM 5 WORKING DAYS
1. Request for data is noted in the work record system
2. Request for data is received
3. Consultation with the applicant is carried out
4. Draft response letter is prepared
5. Draft response letter is checked by quality Assurance officer
6. Response letter is signed by the head of the UDB Management Unit
6a. If request is rejected, reply is delivered by courier
6b. If request is approved, the authorised officer responds with a letter and technical work plan
7. Letter of Assignment is issued
8. Person in charge visits requestry location with response letter and letter of assignment

Source: TNP2K

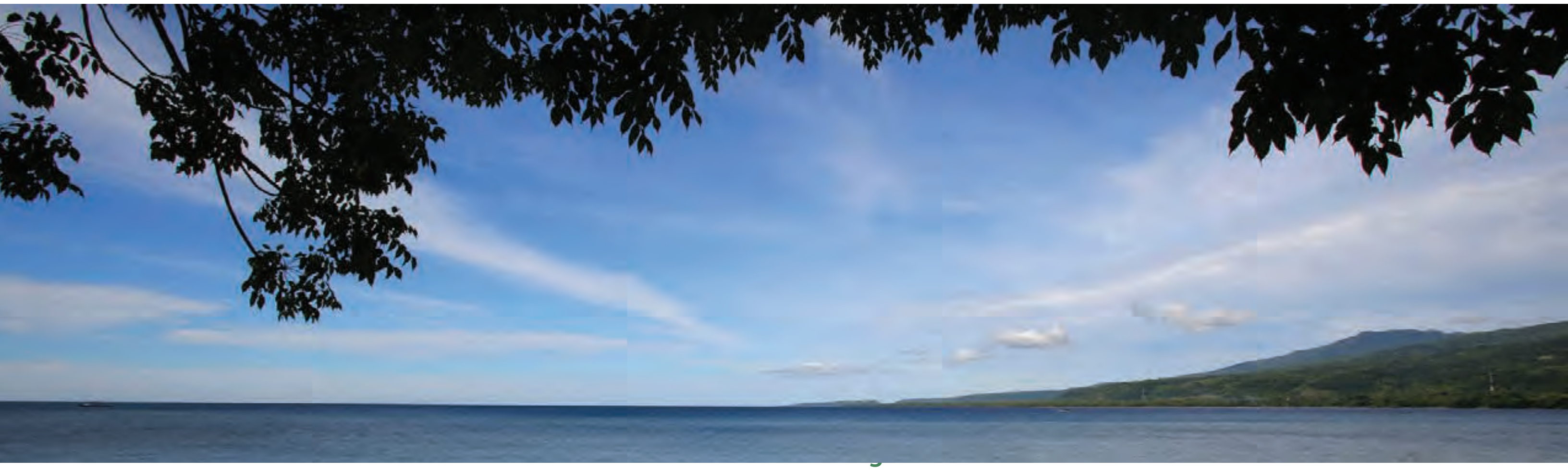


Table 7. Details of the process for handling requests for technical assistance (Figure 6)

Numbered Stages	Stage	Process details
1-2	**A request for technical assistance is received**	a. The applicant seeking assistance sends a letter requesting help. b. The letter is forwarded to the management unit head for follow-up approval.
1-2	**The request for assistance is noted in the work record system**	Applications approved for follow-up are recorded in the work record system
3	**Responsibility for handling the request is assigned to an authorised officer**	The unit head or the authorised officer delegates the follow-up action for handling the data request to a member of the authorised work group.
4-6	**Consultations are held with the applicant requesting technical assistance**	The delegate contacts the applicants or their representatives in order to: - Reconfirm the request for technical assistance - Discuss the details of the assistance to be provided - Explain the process involved and the time required
7	**A letter of reply and technical work plan are drafted**	a. The authorised officer drafts a reply in accordance with the management unit head's requirements b. Depending on whether the head agrees to the request, a letter of work is prepared c. The data quality assurance officer does a final check of the draft reply
8	**Technical assistance is/is not provided**	a. If the applicant's request is rejected, a reply is delivered by contracted courier. b. If the request is accepted the authorised officer replies with a letter that includes the technical work plan.

Source: TNP2K

Requests for technical assistance that have been approved by the management unit head are recorded in the work record system and the appointed delegate arranges for a consultation with the applicant. Consultations generally focus on the technical needs of the applicant.

Next, the authorised officer drafts a reply regarding the request. Once approved and initialled by the data quality assurance officer it is forwarded to the manager for signature. If the request is deemed unacceptable this is communicated directly to the applicant and at this point the request is considered handled. When a request is accepted, a letter of reply is sent by the officer appointed to liaise with the applicant on training and information needs. After that, a specific task list is drawn up. The technical assistance stage is considered completed once the officer has visited the applicant's place of work, delivered the letter of reply and the task list, and completed all the tasks listed. The management unit head does not request payment for any aspect of the technical assistance provided.

DOCUMENTING DATA SERVICES

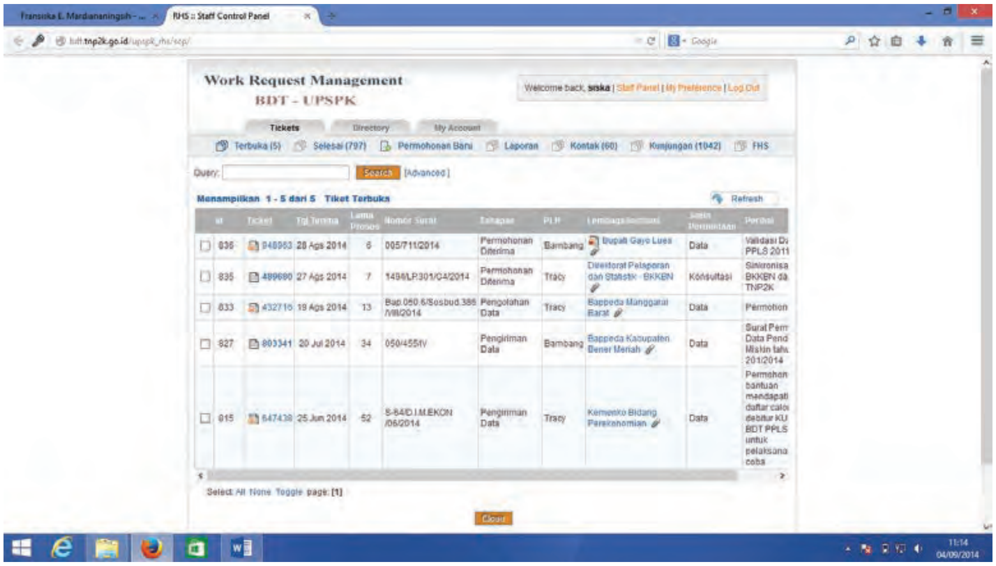
For the purpose of public accountability, the UDB unit records all data services and technical assistance provided, as well as all published data that has been sourced from the UDB. This section details the work record system for documenting data services and technical assistance, as well as the archiving system used to store documents published on data provided by the UDB.

Work record system

The work record system is an information portal for the UDB management unit to track and record communication on requests for data and technical assistance provided. All members of the unit have unique user names and passwords to access the portal. From the portal screen (Figure 7), officers choose which of the following work menus they need:

Menu “Open”	to access information about requests for data or assistance which are still being processed;
Menu “Finished”	to access information about requests for data or assistance that have been processed through to completion;
Menu “New request”	to register new requests for data or technical assistance;
Menu “Report ”	to access reports about requests for data or technical assistance that have been completed or are still being processed;
Menu “Contact”	to access details about applicants requesting data; and
Menu “Visits”	to access reports on face-to-face discussions with potential data users conducted at the UDB office.

Figure 7. Work record system interface



Work Request Management

BDT - UPSPK

Welcome back, siska | Staff Panel | My Preference | Log Out

Menampilkan 1 - 5 dari 5 Tiket Terbuka

	id	Ticket	Tgl Terima	Lama Proses	Nomor Surat	Tahapan	PLP	Lembaga/Instansi	Jenis Permintaan	Perihal
□	836	948963	28 Ags 2014	6	005/711/2014	Permohonan Diterima	Bambang	Bupati Gayo Lues	Data	Validasi Da PPLS 2011
□	835	489680	27 Ags 2014	7	1494/LP.301/C4/2014	Permohonan Diterima	Tracy	Direktorat Pelaporan dan Statistik - BKKBN	Konsultasi	Sinkronisa BKKBN da TNP2K
□	833	432716	19 Ags 2014	13	Bap.050.6/Sosbud.386 /VIII/2014	Pengolahan Data	Tracy	Bappeda Manggarai Barat	Data	Permohon
□	827	803341	20 Jul 2014	34	050/455/IV	Pengiriman Data	Bambang	Bappeda Kabupaten Bener Meriah	Data	Surat Perm Data Pend Miskin tahu 201/2014
□	815	647438	25 Jun 2014	52	S-64/D.I.M.EKON /06/2014	Pengiriman Data	Tracy	Kemenko Bidang Perekonomian	Data	Permohon bantuan mendapati daftar calo debitur KU BDT PPLS untuk pelaksana coba

Select: All None Toggle page: [1]

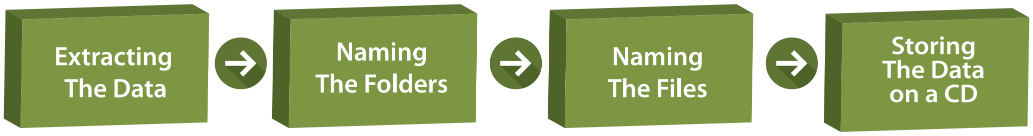
Source: TNP2K

Archiving data

The head of the management unit is responsible for archiving data released to applicants so that all ministries, agencies and local governments remain accountable for data released to them.

At this stage, information extracted from the UDB is termed "ready data". If the ready data has already been checked, the data extractor stores it in the main folder, which contains reference details, information and background details about the data and other relevant reports, all of which are filed according to the details of the applicant. The main folders are kept on the server and in the data backup system. These folders can only be accessed by users with special access approval, according to their functions and duties. The data extractor names the archives by distinguishing between requests for data and requests for technical assistance. The stages for naming the archives are described in Figure 8.

Figure 8. Stages for naming archives



Source: TNP2K

Requests for data or technical assistance are both documented using a follow-up form in the work record system. Any data that is released is given a serial number. This serial number features on the label of the CD containing the data to make it easy to track the data released at a later date. The standard process for applying identity numbers to data is described as:

A. Labelling folders for data and technical assistance requests

- Requests for national data
  National code_Name of ministry or agency_ Request ticket number
  Example: 0_PPN BAPPENAS_ 981234
- Requests for regional data
  Regional code_Name of regency/city_ Request ticket number
  Example: 1607_BANYU ASIN_538789

B. Labelling documents for data and technical assistance requests

- Requests for national data
  National code_ Name of ministry or agency _Name of programme
  Example: 0_PPN BAPPENAS_ RUJUKAN TERPADU
- Requests for regional data
  Regional code_ Name of regency/city _Name of programme
  Example: 1607_BANYU ASIN_BSM DAERAH

C. Labelling CDs for data requests

- Requests for national data
  a. First line:
  Agency or ministry requesting the data
  Example: MINISTRY OF SOCIAL AFFAIRS
  b. Second line: Name of programme
  Example: PKH 2014
  c. Number allocated: CD code_ FTL number/UDB/Month/Year
  Example: 800.561/BDT/VIII/2014

D. Requests for regional data

a. First line:
Name of the province, regency or city that made the data request
Example: Sulawesi Selatan

b. Second line: Name of regency or city
Example: Soppeng

c. Third line: Number allocated
CD code_ FTL number/UDB/Month/Year
Example: 800.561/BDT/VIII/2014

E. Requests for technical assistance

a. First line:

Name of the province, regency or city that made the data request

Example: Sulawesi Selatan

b. Second line: Name of regency or city

Example: Soppeng

c. Third line: Number allocated

CD code_Request ticket number of applicant requesting data/ UDB/ Month/ Year

Example: 800.257608/BDT/VIII/2014

4

The Technology Management System

THE TECHNOLOGY MANAGEMENT SYSTEM

The UDB management unit's system for managing the UDB using information and communication technology (ICT) includes the following:

- Designing a computer network for managing the UDB
- Designing a space to secure the UDB data centre
- Designing ICT services and facilities to support external users of the UDB:

  – Server assistance
  – Application services
  – Network services

- Providing a security system to protect the UDB from unauthorised use and natural disasters
- Developing data management procedures

DESIGNING A COMPUTER NETWORK FOR MANAGING THE UDB

The computer network is an essential part of the ICT system used to manage the UDB and related data sets. Any malfunction in the computer network can severely affect the activities of the management unit so the availability and reliability of the network is critical. Consequently the unit responsible for the network manages it according to the highest international standards.

The network contains redundant capacity components to provide backup, with a single path for power and cooling distribution, and redundant components that ensure 99.7 percent availability. This level of availability exceeds the real time needs of the UDB.

The reliability and availability of the network is managed according to the arrangements shown in Table 8.

Table 8. Ensuring the reliability of the computer network

No.	Description	Implementation
1	**Internet connection failover system**	• Primary internet service provider (ISP): uses a fibre optic connection with a radio link backup connection • Back-up ISP: a second service provider is available should operational problems occur with the primary ISP
2	**Electricity Failover System**	Three-tier electricity failover system: 1. UPS (Uninterruptible Power Supply), 2. Backup electrical generator (genset) installed in the building 3. A genset owned by the UDB management unit

Table 8. Ensuring the reliability of the computer network

No.	Description	Implementation
3	**Vulnerability**	Reducing vulnerability by: • Installing new updates to the operating system (OS) • Installing new updates to antivirus programmes
4	**Firewall**	Configuring the firewall to: • Resist distributed denials of service (DDOS) attacks • Resist FLOOD attacks • Prevent remote access to the internal LAN
5	**Servers**	• Implementing redundant server components (for example, CPU, power supply, fan) • Implementing a server failover system through collocation
6	**Storage**	• Deploying hot swappable disks • Implementing RAID 5 across disks • Using mirrored storage through colocation

Source: TNP2K

Notes: CPU = central processing unit; FLOOD = type of denial of service attack on a computer system; LAN = local area network; RAID 5 = a system of backup drives for extra security.

DESIGNING A SECURE SPACE FOR THE UDB DATA CENTRE

The data centre for the UDB refers to the place where the ICT infrastructure to manage the UDB data and other data sets is housed (including servers, storage devices and other ICT equipment). The room securing the data centre conforms to the following international standards:

ANSI/TIA[5] standards
The ANSI/TIA standards applied in designing and constructing the location for the data include:

– ANSI/TIA-942 telecommunications standards for data centres;
– ANSI/TIA-942-1 data centre coaxial cabling specification and application distances; and
– ANSI/TIA-942-2 telecommunication standards for data centres (addendum 2 – additional guidelines for data centres).

ISO/IEC[6] JTC-1 standards
ISO/IEC standards applied in designing and constructing the location for the data centre included, among others:

– ISO/IEC 24764 Information technology – generic cabling systems for data centres
– ISO/IEC 18010 Information technology – pathways and spaces for customer premises cabling

[5] **ANSI/TIA** (American National Standards Institute/ Telecommunications Industry Association) is an association of companies in the United States that develop industry standards for various types of ICT products. It is a not-for-profit organisation that develops standards based on consensus.
[6] **ISO/IEC JTC 1** is a Joint technical committee established by the International Organisation for Standardisation and the International Electrotechnical Commission to create, maintain, promote and facilitate international standards in the field of ICT.

SERVICE CENTRE

The UDB service centre incorporates the following ICT services:

- Directory services
  In the context of ICT, a "directory" is an information structure that contains a list of users, computers, peripherals and access rights in a computer network. Access to the network is made possible due to the directory service. This service is the basis for a variety of other services, such as:
  - Single sign-on services
  - Roaming user profiles
  - Automatic software distribution and installation
  - Rights management based on computer, clients and properties

- File server
  The file server is a computer connected to a network that provides access to files for laptop computers, workstations and other computers connected to the network. This service allows users to share and exchange files with other users. Managing access rights is an essential part of operating a file server properly, as not all users have access to all files.

- Print server
  The print server allows one or more printers to be used concurrently by one or more users on the network.

- Database server
  The data management unit oversees the UDB and other related data sets, such as Podes (village statistics) and Susenas (National Socioeconomic Survey). Access to the database server is limited to only a few people.

- Application server
  The application server allows software programmes to be used by more than one user simultaneously. Application servers can include:
  - – A server in the network that runs software applications frequently used by network users;
  - – A server running an application or business logic programme in a three-tier architecture allowing interaction between the database server and user access management; or
  - – A web application server that dynamically generates web pages through an internet or intranet connection.

- Mail server
  A mail server or message transfer agent is a computer that handles email within a network. Mail servers are generally used to receive, send and automatically forward email.

- Web server
  The primary function of a web server (HTTP server) is to send the web pages requested by users on a network. UDB data is available to the public through a web site (http://bdt.tnp2k.go.id). The same method of access is provided to UDB staff through the intranet.

APPLICATION SERVICES

Two types of software applications are used to manage the UDB.

- Stand-alone applications
  The simplest form of applications are software programmes stored on the server and loaded into and run on the random access memory (RAM) of the user's computer. This service allows software applications to be executed by the user while the data remains stored on the server.

This service is provided to users who require temporary access to restricted information, such as village-level individual data, for the purposes of assignment related analysis. This access is revoked once users complete their activities.

- Client–server application
  This refers to more complex application software where parts of the programme are launched directly from the server. In the case of the UDB, for example, both the data and the software for managing that data are on the server, and those accessing the

UDB use a single interface. The components on client computers are called 'front ends', which is the software providing the interface to the actual database.

NETWORK SERVICES

The UDB network is accessible in three different ways, depending on who is using the system and why they need the information.

- Intranet
  An Intranet is an organisation's internal network that is available only to employees or individuals granted access approval (for example, staff from ministries, agencies, regional governments, suppliers). Access is controlled by a firewall. As with the Internet, an Intranet is used to share information. Intranets used by the UDB's business units provide various services, including data storage, search and retrieval functions, document sharing and dissemination as well as knowledge management.

- Remote access

  In addition to the internal computer network, limited remote external access to the network can be made available to users who need to work from home or from outside the UDB's main office. For security reasons, remote access is only given on a case-by-case basis. The remote access connection is made through a virtual private network (VPN). VPN connections allow encrypted data to be transmitted, ensuring the data's security while travelling from the server to the client and vice versa.

- Web services

  The UDB management unit provides various web services to accommodate the information needs of other units. These services include providing hosting space, sufficient bandwidth, network security and information services.

DATA SECURITY SYSTEM

Ensuring the security of the UDB is based on three key considerations:

- safety
- quality
- cost

Ensuring data security is a dynamic process whereby periodic reviews examine the need to change systems, technologies and procedures as well as the rules and regulations governing usage.

Policies for managing the security system

The security management system prevents unauthorised access to the UDB data. The system uses best practices, both local and international, as set out in the following management system policies:

- Personnel security policy

  To protect the UDB, the management team have developed a personnel security policy. The key elements in this policy include:

  1. For all new staff, the UDB management unit:
     - Provides the ICT tools the staff member needs to fulfill the job role;
     - Sets up a user account to access the Intranet, Internet, local network, email and other services in line with the duties of the staff concerned;
     - Executes a non-disclosure agreement to protect UDB data and information as well as other related datasets. This agreement is an integral part of the employment contract.

  2. When staff retire or resign the UDB management unit:
     - Retrieves all ICT equipment used by the staff concerned;
     - Disables all of the staff member's user accounts; and
     - Disables all email and instant messaging accounts.

3. Information security awareness programmes are provided regularly for all UDB management unit and the National Team for the Acceleration of Poverty Reduction staff.

All policies concerning UDB management include the following statement:

> **"Any employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment."**

- Freedom of information policy

  Based on Act no. 14 of 2008 on Disclosure of Public Information, the UDB has been classified according to two categories:

  – Public information that the UDB management unit has gathered, stored, managed and/or received through its cooperation with public agencies, as well as other information of public interest.

  – Public information that is exempted from disclosure (such as information that is classified as confidential by law, that contravenes common decency or is against the public interest) is based on a close examination of the potential consequences of making such information openly available and careful consideration of whether the greater good is best served by disclosure or non-disclosure.

The public information policy applied with reference to this law can be summarised as follows:

– Public information is open and can be accessed by anyone seeking it;
– The exclusion of public information from disclosure is limited and tightly controlled.Public Information exempted from disclosure will be provided by the UDB management unit only to users that comply with the applicable legal regulations.

- Data security policy

  The data security policy provides guidelines and recommendations for the creation, storage, handling, reproduction, transmission and destruction of information, especially information that is excluded in the UDB.

  – Data managed by the UDB management unit is stored in a repository;
  – A local repository is used that is physically located within the ICT infrastructure overseen by the UDB management unit and within the territorial area of the Republic of Indonesia;
  – If needed, data can be stored in a private cloud belonging to the UDB

  management unit and within the territorial area of the Republic of Indonesia; and
  - If confidential or restricted information needs to be destroyed, it should be erased physically and electronically.

- UDB asset policy
  Policies governing procedures for accessing the UDB and other related data sets is overseen by the UDB management unit head to ensure the confidentiality, integrity and availability of the database.

  - Full access is given to appropriate database administrators; and
  - Staff within the UDB management unit who require access to the database must coordinate with the database administrator for permission and with the knowledge of the UDB management unit head.

- Policy for access via a VPN (virtual private network)
  The policy for VPN access provides guidance in the management and use of remote access via a VPN connection.

  - VPN access for maintenance of ICT devices from a remote location is only available to authorised personnel, such as the systems administrator and database administrator; and

  - End users cannot have VPN access except in urgent circumstances and with the permission of the UDB chief of data management.

- Security policy for ICT infrastructure
  The ICT security policy provides guidelines and recommendations in the design, development, operation and maintenance of ICT infrastructure.

  - ICT infrastructure must be designed and developed in accordance with the requirements of the UDB management unit head;
  - ICT infrastructure should be procured and maintained periodically by working with authorised dealers and vendors; and
  - ICT equipment is purchased based on local availability, the quality of the after sales arrangements, and the reliability and flexibility of the supplier.

- ICT equipment usage policy
  This policy regulates the use of the equipment owned by the UDB management unit. Indiscriminate usage can result in various risks, such as virus attacks, denials of service and disruptions to computer networks. It can also have legal implications.

  - A laptop computer or device connected to the network must have approved antivirus programmes;
  - Personal computers and laptops in the UDB management unit can only be installed with applications that support the officer’s work and are licensed; and

  - End users are not allowed to install applications on their devices. This must be done through the installation process managed by the system administrator.

- Policy for using mobile devices

  This policy provides guidelines and recommendations on the use of mobile storage and computing devices that access or store information in the UDB management unit.

- Policy for removable storage

  This policy governs the use of removable storage media to minimise the risk of losing data or exposing data that is exempt from disclosure to computer viruses and malware infections. This includes:

  - The use of encryption on removable storage devices;
  - The control of removable storage media through a single integrated interface; and
  - The scanning of removable storage media and personal devices for malware and viruses.

- Server security policy

  The server security policy documents how internal server devices owned or operated by the UDB management unit should be configured:

  - Servers are protected with antivirus programmes and firewall applications;
  - The operational server that manages the UDB cannot be reached via remote access;
  - Servers cannot be accessed directly on-site by end users, except by the system administrator and/or database administrator assigned by the UDB management unit;
  - Other staff requiring direct access to an on-site server must have permission from the appropriate unit manager or the assigned system administrator; and
  - Details of the user account and password for the administration server are strictly limited to the assigned system administrator and should not be removed or made available to others.

- Website development policy

  This policy contains guidelines and recommendations on the design, development, operation and maintenance of websites by the UDB management unit.

- Email policy

  This policy regulates email practices within the UDB management unit. It is intended to safeguard the public image of the management unit, as members of the public sometimes consider emailed information as official statements of policy.

  - Communications that contain information and other official activities regarding the UDB must use the UDB management unit's email programme; and
  - Emails must conform to a standard signature format.

- Internet use policy
  The internet use policy regulates how the Internet should be used within the UDB management unit. Indiscriminate use of the Internet can result in exposure to risks such as viruses, malware attacks, denials of service and disruptions to computer networks. Legal requirements also apply.
  - Internet usage is only allowed for activities that support the work and aims of the UDB management unit; and
  - Internet access is managed by filtering and blocking websites suspected of having viruses, malware, pornographic material, gambling and other content considered offensive or inappropriate.
- Password usage policy
  The policy on the use of the passwords includes guidelines and recommendations concerning protecting and changing passwords:
  - Passwords must have a minimum length of eight characters, consisting of uppercase and lowercase letters, numbers and non-numeric characters; and
  - Passwords should be changed at regular intervals.
- Encryption policy
  Encryption encodes data so it cannot be read directly. The encryption policy provides guidelines on the use of algorithms to encode data to protect it from unauthorised access:
  - The algorithms used are limited to those that have had widespread public review and are proven to work effectively.

Operational procedures

A number of operational procedures are implemented by the UDB management unit:

- **Procedure for using firewalls**

  Access control mechanisms are deployed to support the implementation of policies related to security systems and computer networks.

- **Procedure for securing network servers**
  - Apply "CIA Triad" principles:
    1. Confidentiality— safeguarding the confidentiality of information stored on the server;
    2. Integrity— safeguarding the integrity of information stored on the server; and
    3. Availability—safeguarding the availability of services provided by the server;
  - Maximise the security of all network servers; and
  - Be alert to all threats to server security and restore servers should a security breach occur.

- **Procedure for securing public Web servers**
  - Install safe servers; and
  - Configure the Web server software and operating system.

- **Procedure for securing desktop workstations**
  - Generally adopt the same procedure as for securing a server network.

- **Procedure for detecting signs of intrusions**
  - Collect and review information to: detect any intrusion; determine the data, systems and networks that have been attacked; as well as to detect the nature of the attack (confidentiality, integrity, availability of services).

- **Procedure for responding to intrusions**
  - This includes the steps for restoring the data and the system to its original state.

Physical security system

In general terms, the physical security system deployed includes:

- **Defining the physical perimeters** necessary to protect specified areas, such as offices, data centres and UDB facilities.

  Actions to protect the physical office space of the UDB management unit include:
  - Deploying security guards;
  - Using security cards to allow entry to the premises;
  - Using different security cards to enter the office space of the UDB management unit;
  - Using double doors equipped with airlock systems at the entrance of the UDB management unit's office space;
  - Operating closed-circuit television (CCTV) around the clock.

- **Providing physical controls** for certain areas, such as locks, doors with air-lock system, finger print scanners, and so forth.

The data centre within the UDB management unit office area is equipped with:

- Steel plated walls;
- An entrance door with biometric security protection (fingerprint) as well as manual controls;
- Restrictions on those who can enter the area, as determined by their job requirements; and
- Smoke detectors and automatic fire extinguishers.

- **Protecting information** and related data facilities from natural calamites and threats from external parties.

  Data storage media, UDB data and other data sets are protected by:
  - Policies and procedures for the management of removable media;
  - Policies and procedures for the disposal and destruction of printed information; and
  - Policies and procedures for the exchange of data using removable media.

- **Establishing control protocols for work activities in protected areas.**
- **Preventing access by unauthorised persons.**

Disaster recovery plan

Disasters are events that are usually unpredictable and often highly destructive. Different types of disasters may include:

- Disasters resulting from geographical and geological conditions;
- Fires due to environmental factors or faulty electrical systems;
- Disruptions to electrical supplies due to problems with the power grid;
- Damage to equipment and systems due to malfunction or human error;
- Attacks by a virus that damages devices, systems or data; and
- Terrorists attacks.

Such disasters may disrupt or suspend the operation of systems used by the UDB management unit. The UDB management unit head has developed a disaster recovery plan policy that includes:

- **A computer emergency response plan**
  - Who needs to be contacted, when and how?
  - What steps need to be taken in the event of an emergency?

- **Staff succession plan**
  - The procedures to follow if specific staff are not in place or can not carry out their duties.

- **Data study**
  - Information about the data stored in the system, their levels of importance, as well as their levels of confidentiality.

- **List of critical services**
  - The services provided by the UDB management unit and their order of priority. A recovery order is also provided, for both short and long term.

- **Data backup and restoration plan**
  - The mandatory procedure for backing up data, the backup media used, where the media is stored and how often the data should be backed-up. Information on how to retrieve the backed-up data is also provided.

- **Equipment replacement plan**
  - Describes the equipment used to provide services, the process for ordering equipment, and where it can be purchased.

- **Managing the mass media**
  - Clarifies who is authorised to provide information to the media and the type of information that can be provided in the event of an emergency.

DATA MANAGEMENT PROCEDURES

Data cleaning

Data cleaning or data scrubbing is the process of detecting and correcting (or removing) corrupt or inaccurate records from a record set, table or database. Used mainly in databases, the term refers to the identification of incomplete, incorrect, inaccurate or irrelevant elements in a data set and then replacing, modifying or deleting defective data (Wu 2013).

Data cleaning is a management responsibility and is performed by the UDB management unit following the handover of data. The criteria and devices used in managing data quality comprise:

- **Validity:** This is the criteria used to determine the validity of data provided to the UDB management unit, based on the nature or type of data received. Validity criteria include:

  - Testing data-type constraints: deciding if the type of data provided is appropriate;
  - Testing range constraints: checking that data content does not exceed the determined minimum or maximum values;
  - Testing mandatory constraints: determining if obligatory data has been prepared correctly;
  - Testing unique constraints: checking if the unique identifiers for data rows are correct;
  - Testing foreign-key constraints: ensuring the reference details for data rows are aligned with the reference list;
  - Testing regular expressions: specifying whether text content conforms with format requirements (for example, addresses or ID numbers); and
  - Testing cross-field validation: checking if a data combination conforms to allowed configurations.

- **Accuracy:** This refers to determining the accuracy of data received compared with actual field conditions. The UDB management unit undertakes the following steps to determine the accuracy of the data it receives:

- Performing direct examinations (spot-checks) in the field or other random sampling of the received data; and
- Checking the existence of specific data by cross-checking it with other data, for example other databases or data sets containing demographic, health, educational, financial and other information. This is facilitated through data matching activities.

- **Completeness:** This refers to how complete the data is according to its description. The UDB management unit may investigate the existence of certain data on the basis of other data, for example, other databases or data sets containing demographic, health, educational, financial and other data. Data resulting from this examination may be used to supplement other data received by the UDB management unit.

- **Consistency:** This includes criteria for determining the consistency of rows of data across the entire content of data received. Only data with a high level of consistency or data which can be improved are processed.

- **Uniformity:** This refers to the criteria for determining the overall level of uniformity of the data received. Data received is processed to ensure it is stored according to the parameters required by the UDB.

The above criteria are used by the UDB management unit to detect errors in the data it receives and to make any necessary corrections. Applying the above criteria may involve all or some of the following:

- **Parsing:** This activity detects whether the contents of the data can be read according to the requirements specified in its accompanying description. Parsing analyses the received data for errors.

- **Data transformation:** This activity moves and formats data according to the database management application used by the UDB management unit. This process also converts and normalises data that may contain errors or does not comply with existing information.

- **Duplicate elimination:** This refers to deleting duplicated data rows. The UDB management unit is required to delete 100 percent of all duplicate data to reduce the risk of losing data that is valid.

- **Statistical methods:** These include determining the mean, standard deviation, range and clustering algorithms. The process involves cross-referencing the statistics of other equivalent databases to locate errors. Statistical methods can also be used to improve the content of the data through other data values that have been through augmentation, algorithm analysis and extensive cross-referencing.

At the completion of the data cleaning process the UDB management unit can determine the utility of the data received and whether it can be used in its entirety or only partly, based on the above criteria.

Data filtering

Data filtering or Information filtering is a system that removes redundant or unwanted information from an information stream using (semi)automated or computerised methods before it reaches a human user. Its main goal is to manage information overload and signal-to-noise ratio. To do this, the user's profile is compared to specified characteristics. These characteristics may originate from the information itself (the content-based approach) or the user's social environment (the collaborative filtering approach) (Hanani, Shapira and Shoval 2001: 203–259).

Filtering is undertaken by the UDB management unit to ensure the data it provides meets the needs of the user. Filtering actions include:

- **Requirement analysis:** This activity determines the needs of the data request. It provides information about the range of data required in the next step, namely:
  - Data classification: Determining the required data classification, including the type of data entities (households and individuals), the level of aggregation (details concerning specific data attributes) and the data's level of confidentiality (with or without names and addresses);
  - Area: Determining the required data limits in the region based on the division of administrative regions in Indonesia;
  - Time: Determining the limits of validity of the data based on the range of data required;
  - Entity attributes: Specifying data constraints according to the attributes of the information available (for example, gender of household head or types of jobs); and
  - Data format: Specifying the type of electronic data format that can be used to accommodate the results of the data filtering process.

- **Filter formatting:** This activity prepares the filter according to a format that can be executed by the computer device used by the UDB management unit. This process can be done automatically or semi-automatically depending on the complexity of the needs assessment.

- **Data transformation:** This activity formats the filtered data according to the requirements of the analysis.

Data matching

Data matching is the task of identifying, matching and merging records that correspond with the entities or data fields used in other databases. These data fields or entities usually include people, such as patients, customers, tax payers or travellers, but they can also refer to publications or citations, consumer products or businesses. A special situation arises when trying to find records that refer to the same entity within a single database, a task commonly known as duplicate detection. Over the past decade, various application domains and research fields have developed their own solutions to the problem of data matching and as a result this task is now known by many different terms. Besides data matching, the terms most prominently used are record or data linkage, entity resolution, object identification or field matching (Chisten 2012).

Data matching is carried out by the UDB management unit to meet the requirements of specific data. The UDB management unit performs the following matching procedures:

- **Data pre-processing:** This step ensures that any data to be matched with the UDB is prepared in a format compatible with the data processing device that the management unit uses. The ensuing processing activities are then executed on the same device.

- **Indexing:** This step is done to reduce the complexity resulting from the data matching process and to build an effective index structure that can potentially generate matching data. This step can involve the selection of the data column to ensure data can be compared and matched.

- **Record pair comparison:** This step runs matching algorithms on the index structure compiled in the previous step. The matching algorithm is used for referencing purposes:

  - Exact match: These algorithms compare the contents of the data to ensure an exact match;
  - Approximate match: These algorithms compare the contents of the data to ensure similarity. Some of the algorithms used include: Levenstein distance, Jaro–Winkler distance and regular-expression comparison; and
  - Triangulation confirmation: These algorithms examine the connections between different matching algorithms run on the data. They allow more specific classification of the data.

- **Classification step:** This step places matching data into different groups, depending on the decision model applied. Common groupings include:
  - Matches: the pairs of data in both databases are considered equal. Generally they are divided into:
    - Hard matches: Exactly matching data. This is generally considered the best result an exact match algorithm can deliver.
    - Soft matches: Very similar data. Generally this is the best result possible from using a combination of approximate match algorithms and triangular confirmation. To facilitate decision making the results are usually presented in a similar gradation based on the number of matching algorithms that were run on the data.
  - Non-matches: This is all the data found that does not match with the UDB data. It may include data that is entirely different or soft-match data subsequently determined as non-matching.

- **Evaluation step:** This is the point where the results of the matching activities are assessed. This step determines any improvements that can be made based on each of the matching activities carried out by the UDB management unit.

Archiving and tracking released data

The UDB management unit archives and tracks released data in stages to protect data processing results from potential damage and to ensure the results are searched and checked, if required.

The UDB management unit carries out several activities for referencing purposes:

- Documenting in hard copy the entire data request process;
- Keeping a soft copy on a file server that documents the entire data request process;
- Recording the data request process in the work request database;
- Storing all the scripts/programmes run by the data processing devices on the file server managed by the UDB management unit;
- Storing records of the processes undertaken and results achieved on the database managed by the UDB management unit; and
- Keeping copies of electronic files on the file server.

The UDB management unit also ensures that files on the file server and database server are backed up according to the disaster recovery plan policy.

5

Handling Complaints and Updating the UDB

COMPLAINTS HANDLING SYSTEM

The main purpose of the complaints handling system is to better respond to the needs of stakeholders – these include the beneficiaries or potential beneficiaries of social protection programmes as well as government and non-government agencies and other institutions involved in planning and implementing such programmes. The specific aims of the complaint handling system include:

- Responding quickly and effectively to complaints or concerns about the targeting of programme participants;
- Supporting social protection programmes in implementing transparency, openness, public participation and accountability; and
- Updating the UDB and reducing inclusion and exclusion errors in social protection programmes membership.

However, minor updating of programme participants is sometimes carried out by the programme manager, not by the UDB management unit.
Complaints are handled according to the following principles:

- **Simple and easy to access:** The procedure for submitting complaints and responding to them has been simplified so that it is better understood and more readily used by stakeholders. Complaints can be submitted in several ways (as described in the next section).
- **Transparent:** Information about the complaints handling system has been widely disseminated to governments, agencies and communities across Indonesia.
- **Handling time:** Complaints handling must meet specified deadlines, starting from the receipt of the complaint through to its resolution. These deadlines are determined by the UDB management unit based on the nature and complexity of the issue.
- **Right to appeal:** Channels for making appeals have been made available for complainants dissatisfied with the decision made regarding their grievance.
- **Confidentiality:** The identity of people making complaints is kept confidential unless they have requested otherwise.
- **Accountability:** Any officer associated with handling a complaint must adhere to specific roles and responsibilities, and may be monitored, both internally and externally (including by civil society organisationss and the media).
- **Fairness:** Each complaint is handled according to the same procedure regardless of the person filing the complaint or the person who may be the subject of the complaint.

The steps in the complaints handling system are as follows:

- A complaint is submitted;
- The complaint is recorded in the information management system;
- Details about the complaint are sought and a decision reached; and
- A response or decision is provided.

Each of these steps is clarified below:

- A complaint is submitted
  Complaints can be submitted in several ways:
  - Delivered directly by the individual, family or household by completing the complaints form and sending it to the UDB management unit;
  - Delivered indirectly (through an implementing agency or the local poverty reduction coordination team). For example, an individual, family or household may feel they are entitled to participate in a programme but they are not included in the list of beneficiaries published by the UDB. People in this situation can consult with the managers of the programme in their area or with the local team as well as get assistance in filling in a complaints form and sending it to the UDB management unit.
  - Other ways might include a local government or non-govermental organisation identifying groups in the community who are excluded from the programme.

- **The complaint is recorded in an information management system**

  Recording complaints can be done in several ways:

  - Directly with the UDB management unit;
  - Through parties implementing a programme at the central or regional level; and
  - Through a mobile application especially developed for submitting complaints to the complaints handling system management.

- **Details about the complaint are sought and a decision reached**

  Getting details about the complaint involves:

  - Reviewing the thoroughness and validity of the documents related to the submitted complaint;
  - Performing data matching with the UDB to verify whether or not the individual, family or household submitting the complaint has been recorded in the database. This can be carried out by implementing programmes in those regencies or cities that have the capacity to conduct matching queries with the UDB. To do this the implementing programme must have the relevant data about the individual, family or household concerned, including the relevant variables, in order to match data with the UDB.
  - Using the decision-making process shown in Table 9.

- **A response or decision is provided**

  Responses and decisions regarding complaints – in particular those concerning inclusion and exclusion errors – are coordinated by the UDB management unit and the programme providers to ensure the information is consistent and that solutions are delivered according to the policies and decisions of the programme organisers concerned.

Table 9. Decision-making process in the UDB's complaints handling system

Type of complaint	Information	Decision-making process
1. Excluded from the list of programme beneficiaries	The individual, family or household is not included on the list of beneficiaries for the following reasons: 1. The household submitting the complaint has not been surveyed and therefore is not recorded in the UDB. 2. The household submitting the complaint is recorded in the UDB but does not qualify as a beneficiary according to the criteria used by the implementing programme. 3. There has been a mistake in determining the household's welfare	1. Information about the complainant is sought in the UDB 2. If the individual, family or household making the complaint is not recorded in the UDB, then: a. Information is submitted to the programme organisers. The decision to enter or not enter the individual, family or household's details into the UDB is under the authority of the programme organisers. b. The data for the individual, family or household making the complaint is kept on a list of target data for possible use in future UDB updates. 3. If the complainant household is in the UDB but did not qualify as programme beneficiaries, an explanation is sent to the parties concerned.
2. An individual, family or household is not receiving benefits provided by the programme despite being on the list of recipients	This situation can occur because: 1. Programme organisers may include participants from their own list who are not in the UDB thereby filling a preset quota. 2. A mistake in determining the household's welfare status has occurred due to a data collection error.	1. Information about the complainant is sought in the UDB. 2. If the complainant is not recorded in the UDB, the UDB management unit will inform the programme managers. A response will also be sent to the complainant, in line with the polices of the programme concerned. 3. If the complainant is registered in the UDB and qualifies as a beneficiary, clarification is sent to the complainant and the programme organisers .
3. The number of households entered in the UDB for a specific area is lower than the number of people considered poor and entitled to participate in a government social protection programme.	The complainant claims that a list of households in a specific area contained in the UDB fails to acknowledge their level of poverty.	1. A check is made of the poverty incidence quota for the areas complaining (using the poverty map from the population census and/or data from Susenas) and calculated against the quota of households that should be recorded for the areas concerned. 2. If the number of households in the UDB for the area concerned is less than the quota: a. The UDB management unit asks the complainant to provide data about the households on a complaints submission form. b. A survey of the above-mentioned households is conducted using the UDB update process 3. If the number of households for the region is higher than the quota, the UDB management unit advises on the number of households assessed and provides a brief explanation to the complainant of the criteria used by the UDB to determine which households are poor

Table 9. Decision-making process in the UDB's complaints handling system

Type of complaint	Information	Decision-making process
4. An individual, family or household is not considered entitled to participate in the programme but is included in the list of beneficiaries.	This situation can arise because: 1. Programme organisers may include participants from their own list who are not in the UDB. 2. A mistake in determining the household's welfare status has occurred due to a data collection error.	1. Information about the complainant is sought in the UDB 2. If the complainant is not recorded in the UDB, this information will be forwarded to the programme organisers. The response to the complainant will be in line with the response from the programme organisers. 3. If the household making the complaint is recorded in the UDB and qualifies as a programme beneficiary, an explanation is provided to the complainant and the programme organisers.
5. Complaints about the UDB services provided by the UDB management unit.	The complainant (a household, programme or other) claims that staff in the UDB management unit fail to provide UDB-related services in accordance with the published procedures for issuing data.	1. The complaint is recorded in the information management system by the UDB management unit. 2. An internal review is initiated. 3. The UDB management unit sends a response in accordance with the findings of the review.
6. Complaints about programmes using the UDB.	The complainant expresses dissatisfaction with a programme using the UDB – not about the targeting (for example, an operational problem).	The complaint is recorded in the information management system by the UDB management unit and forwarded to the programme organiser.

UPDATING THE UDB

Activities to update the UDB are undertaken with the following objectives:

1. Updating UDB's household data to match current conditions. Such data updates may include changes in the location of the household's domicile, deaths or births or changes to the number of household members, changes to the names of household members according to population administration (Adminduk), completing data for the population identity number and family cards (*Kartu Keluarga*), adding information about current participation in social protection programmes, as well as household socioeconomic data (employment, education, physical state of the house, asset ownership, and so on).

2. Improving the effectiveness of targeting social protection programmes to reach poor households not included in the UDB.

There is no specific time limit for updating the UDB. The timing for updates needs to consider the dynamics and changes in household conditions, factors that may affect public engagement (e.g. government election activities), the readiness and support of the local government to coordinate activities as well as the capacity of the local government budget. UDB updates can be performed simultaneously on all targeted households as an intermittent activity, or as a continuous process in line with the system of handling complaints concerning programme participation.

By 2015, the Government of Indonesia had implemented a simultaneous update on all targeted households in the UDB. The update was conducted in two phases, a public consultation stage and a data collection stage. During the public consultation phase, the list of households registered in the UDB was verified through a Public Consultation Forum (FKP - *Forum Konsultasi Publik*) consisting of village chiefs, chair persons of neighborhoods and hamlets, and religious and community leaders. The FKP indicated which households had moved domicile or were considered either in need or not in need of social assistance. The subsequent list of households verified by the FKP was then approved by the head of the local area (e.g. District Head, Regents, Mayors) and included on the list of households to be targeted in the data collection stage.

The documenting of households was conducted by a team of assessors trained and coordinated by Statistics Indonesia (BPS - *Badan Pusat Statistik*). At the time of the data collection, officials also conducted consultations with poor households and through ad-hoc 'sweeping' of areas, as was done at the time of PPLS 2011, to identify disadvantaged parties not included in the FKP's verification results. In the course of updating the UDB in 2015, a number of socioeconomic indicators for households were added to complement the indicators used in PPLS 2011. The indicators added included, among others, the ownership of paddy fields and livestock as well as business turnover. The addition of indicators was done to better analyse a household's level of welfare, as well as to accommodate the needs of social protection programmes in their selection of the target beneficiaries.

Further updates to the UDB are expected to be implemented on a continuous basis, consistent with the complaints handling system. The continuous updating of the UDB occurs through a process that triggers an update whenever there is a report or complaint regarding the data entry for a household/family/individual on a government-run social protection programme's list of participants or beneficiaries. Reports / complaints are handled through the following sequence of activities:

1. Checking the data for households/families/individuals in the UDB.
2. Confirming if the household/family/individual is/are already registered in the UDB.
3. Confirming if the data on household/family/individual in question conforms with the criteria for participation established by the programme.
4. For a household/family/ individual that is confirmed as not registered with the UDB (activity number 1), secondary data is collected to verify they are in fact poor and underprivileged. Secondary data may include advice from the Neighborhood Head for the area concerned.
5. Based on the results of verifying if a household/family/individual is eligible (activity number 4), they are assessed for inclusion in the UDB using the same tools and methods applied in the 2015 update to the UDB.

6. Household data obtained in the activity number 5 is entered into the UDB and is used to analyze household welfare levels and establish whether the conditions of households/families/individuals concerned are in accordance with the criteria for programme beneficiaries.
7. The results of the analysis (activity number 6) are submitted to the agency organizing the programme for their consideration when making decisions regarding which households/families/individuals can participate in their programme.

The involvement of local governments, particularly the TKPK, is very important in the implementation of the Complaints Handling System and continuous updating of the UDB. The main role of local governments / TKPK is expected to be one of verifying, in stages, the eligibility of households as poor or vulnerable as well as coordinating the delivery of the outcome of any complaints lodged with the Complaints Handling System to the households/families/individuals concerned.

References and Annexes

REFERENCES

Bappenas. 2010. Evaluation of Family Planning Services for the Poor. Bappenas, Indonesia. Accessed September 4, 2014, http://www.bappenas.go.id/files/3513/4986/1937/laporan-akhir-evaluasi-28-jan-1__20110512124617__1.pdf

Christen, P. 2012. Data Matching: Concepts and Techniques for Record Linkage, Entity Resolution and Duplicate Detection. Berlin and Heidelberg: Springer-Verlag. Government of Indonesia. 2010. Medium-term National Development Programme Phase II (2010–2014). Jakarta: Government of Indonesia.

Hanani, U., B. Shapira and P. Shoval. 2001. "Information Fltering: Overview of Issues, Research and Systems". User Modeling and User-Adapted Interaction 11(3):203–259.

Imawan, W. 2008. Pendataan Program Perlindungan Sosial PPLS 2008. Presentasi dalam Rapat Koordinasi Tingkat Nasional Program Bantuan Langsung Tunai untuk Rumah Tangga Sasaran. Cikampek, 4 Juni.

Lockley, A, J. Tobias and A. Bah. 2013. Hasil Kajian Gender dari Basis Data Terpadu (Results of the study on gender and the Unified Database). Jakarta: National Team for the Acceleration of Poverty Reduction.

Ritonga, H. 2014. Pengembangan dan Pemanfaatan Data Kemiskinan dengan Bertumpu pada Kebijakan serta Ruang dan Peluang Pihak Lainnya, Presentation at the National Workshop: Participatory database and interactive application for mapping socioeconomic characteristics, and Administration Information Systems (Villages and Urban Wards), Jakarta, 27 Februari 2014

SMERU. 2006. Rapid Appraisal of the Implementation of the 2005 Direct Cash Transfer Program in Indonesia: A Case Study in Five Kabupaten/Kota. Research Report. Jakarta, Indonesia: SMERU Research Institute.

Sumarto, S., A. Suryahadi and W. Widyanti. 2002. "Designs and Implementation of Indonesian Social Safety Net Programmes". The Developing Economies 40(1): 3-31.

TNP2K.2015. A Single Registry for Targeting Social Assistance in Indonesia, TNP2K 2015: Lessons from the establishment and implementation of the Unified Database for Social Protection Programmes. TNP2K, Jakarta, Indonesia.

Widianto, B. 2012. Pengelolaan dan Pemanfaatan Basis Data Terpadu untuk Program Perlindungan Sosial (The management and use of the Unified database for Social Protectino Programmes) TNP2K Secretariat Presentation, Jakarta, January 2012.

Wu, S. 2013. "A Review on Coarse Warranty Data and Analysis", Reliability Engineering and System Safety 114: 1–11.

Annex 1: Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE NATIONAL TEAM FOR THE ACCELERATION OF POVERTY REDUCTION

AND

THE MINISTRY OF AGRICULTURE'S FOOD SECURITY AGENCY

NUMBER ……….

NUMBER ………..

REGARDING
COOPERATION ON THE USE OF NAMES AND ADDRESSES FROM THE UNIFIED DATA BASE (UDB) FOR THE IMPLEMENTATION OF SOCIAL WELFARE PROGRAMMES.

……………

On this day ……, dated ……. month ……., year ……., in Jakarta and signed below:

I. BAMBANG WIDIANTO, as the Deputy Secretary to the Vice President - People's Welfare and Poverty Reduction and in his role as Executive Secretary for the National Team for the Acceleration of Poverty Reduction (TNP2K - Tim Nasional Percepatan Penanggulangan Kemiskinan) located in and operating from Jalan Kebon Sirih Nomor 14 Jakarta 10110, is acting to respect this MOU for and on behalf of the National Team for the Acceleration of Poverty Reduction, and is hereafter referred to as the "FIRST PARTY".

II. ……………………….., located in and operating from ……………….., to respect this MOU is acting according to his/her role both for and in the name of ………………., and is hereafter referred to as the "SECOND PARTY".

THE FIRST AND SECOND PARTIES are hereafter collectively referred to as "THE PARTIES".

For the purpose of clarification, "THE PARTIES" affirm:

1. That the "FIRST PARTY" is the agency responsible for cross-sectoral and cross-stakeholder coordination at the central level aimed at accelerating poverty reduction, and includes the management of the UDB and its role in assisting social protection programmes.

2. That "SECOND PARTY" is ....
3. That in order to carry-out ...., the "SECOND PARTY" requires information and data from the UDB regarding ....

"THE PARTIES" agree that:

Article 1
DEFINITION

Within this Memorandum of Understanding, unless specified by another word beginning with a capital letter, words commencing with capital letters have the following meanings:

1. **Unified Data Base (BDT - Basis Data Terpadu) is the integrated, collected data on target households obtained from the 2011 Social Protection Data Collection (PPLS 2011), as well as data processed by the "FIRST PARTY", that has been entered into the UDB. Among other details, the UDB contains information about target households.**
2. **BPS is Statistics Indonesia (Biro Pusat Statistik Republik Indonesia).**
3. **RTS or Rumah Tangga Sasaran is the beneficiary household targeted by the social protection programme.**
4. **RTS Data is information about the names and addresses of beneficiary households obtained from the Social Protection Data Collection Programme.**
5. **PPS (Program Perlindungan Sosial) are social protection programs implemented by the Government of the Republic of Indonesia to alleviate poverty in the country.**
6. **....... (description of the program or activity that will use UDB data containing names and addresses)................................**

Article 2
SCOPE OF COOPERATION

"THE PARTIES" agree to cooperate in their use of the UDB, which is maintained by the "FIRST PARTY", to implement .... (name of the program that will use UDB data)

Article 3
RESPONSIBILITIES OF "THE PARTIES"

(1) "THE FIRST PARTY" is responsible for making available data about target households that .... (criteria of the targeted household required by the program or activity)

(2)"THE SECOND PARTY" will use the target households data provided by the "FIRST PARTY" to conduct .... (name of the program or activity)

(3) The "SECOND PARTY" is responsible for guaranteeing the security and confidentiality of houshold data provided by the "FIRST PARTY" and for ensuring that data is not used by employees, agents, consultants or contractors engaged by the SECOND PARTY for purposes other than for monitoring program management and state financial responsibilities in carrying out social protection programmes by national ministries and agencies.

Article 4
COOPERATION TIME-FRAME

(1) The MOU is valid for one year, commencing on the day and date of signing by "THE PARTIES".

(2) The time-frame noted in the MOU can be extended based on a signed between "THE PARTIES".

Article 5
CLOSURE

(1) This MOU has been produced and signed by "THE PARTIES" in sincere and good faith, and made in duplicate for each party, with each having the same binding and legal force.

(2) Any matters missing or insufficiently covered in the MOU will be determined through agreement between "THE PARTIES" and set forth in writing in the form of an addendum and considered an integral part of the MOU.

The above Memorandum of Understanding has been produced, agreed to and signed by "THE PARTIES" for use in a fit and proper manner.

Deputy Secretary to the Vice President - People's Welfare and Poverty Reduction and Executivy Secretary for the National Team for the Acceleration of Poverty Reduction	....
TNP2K	....
Bambang Widianto	....

Annex 2: Information about the programme

INFORMATION ON REGIONAL GOVERNMENT USE OF THE UNIFIED DATA BASE IN SOCIAL PROTECTION PROGRAMMES

STAFF CONTACT DETAILS

Name :
Position :
Agency/office :
Office phone :
Mobile phone :
Email address :

PROGRAMME DETAILS

Description: If there is more than 1 (one) programme requiring target data from the UDB, please specify each programme using the same format as below.

Programme Name : ____________________________
Agency/office
(SKPD) Programme Managers : ____________________________
Intended aim or benefit
of the programme : ____________________________

Criteria for programme's
target beneficiaries : individual family household
(please the choice according to the program's aims)

(please detail the target characteristics) ____________________________
____
____
____
____

Total number of
programme beneficiaries : ____________________________

(Place and date),

(Name, signature, official seal/stamp of the Regional Head or Deputy Regional Head as the Chair of the Regional Poverty Reduction Team (TKPKD - Tim Koordinasi Penanggulangan Kemiskinan Daerah (TKPKD)

Annex 3: Affidavit confirming responsibility for protecting data integrity

DECLARATION OF FULL RESPONSIBILITY FOR PROPER USE IN SOCIAL PROTECTION PROGRAMMES OF ANY DATA FROM THE UDB CONTAINING NAMES AND ADDRESSES

The undersigned affirms the following:

1. Agrees to use information provided by TNP2K from the Unified Data Base (UDB) to implement ……....... (name of programme) in ....… (name of location/area)
2. Agrees to protect the confidentiality of UDB data containing names and addresses and to use this data only in accordance with the needs of the programme described in point one.
3. Will not hold TNP2K in any way responsible for any claim, lawsuit or damages laid against TNP2K resulting from the use of data containing names or addresses in a manner that does not comply with the usage requirements defined in this statement.
4. Agree to destroy all documents and any other information from the UDB containing names and address as soon as the programme mentioned in paragraph 1 is completed.

(Place and date

(Name, signature, official seal/stamp of the Regional Head or Deputy Regional Head as the Chair of the Regional Poverty Reduction Team (TKPKD - Tim Koordinasi Penanggulangan Kemiskinan Daerah (TKPKD)

NATIONAL TEAM FOR THE ACCELERATION OF POVERTY REDUCTION

Secretariat of the Vice President of the Republic of Indonesia
Jl. Kebon Sirih No. 14 Jakarta Pusat 10110
Phone : (021) 3912812
Fax : (021) 3912511
E-mail : info@tnp2k.go.id
Website : www.tnp2k.go.id

♻ Printed on recycled paper

ISBN 978-602-275-159-5
9 786022 751595 >