Implementation of the Data Seal of Approval

The Data Seal of Approval board hereby confirms that the Trusted Digital repository DHS Data Access complies with the guidelines version 2014-2017 set by the Data Seal of Approval Board.
The afore-mentioned repository has therefore acquired the Data Seal of Approval of 2013 on August 18, 2014.

The Trusted Digital repository is allowed to place an image of the Data Seal of Approval logo corresponding to the guidelines version date on their website. This image must link to this file which is hosted on the Data Seal of Approval website.

Yours sincerely,

The Data Seal of Approval Board

Assessment Information

Guidelines Version: 2014-2017 | July 19, 2013
Guidelines Information Booklet: DSA-booklet_2014-2017.pdf
All Guidelines Documentation: Documentation

Repository: DHS Data Access
Seal Acquiry Date: Aug. 18, 2014

For the latest version of the awarded DSA   http://assessment.datasealofapproval.org/seals/
for this repository please visit our website:

Previously Acquired Seals: None

This repository is owned by: **CentERdata**
Tias Building
Warandelaan 2
5037 AB Tilburg
The Netherlands

T +31 13 466 8325
F +31 13 466 8326
E CentERdata@uvt.nl
W http://www.centerdata.nl/

Assessment

0. Repository Context

Applicant Entry

Self-assessment statement:

First launched in 1993, the DNB Household Survey (DHS) supplies longitudinal data to the international academic community, with a focus on the psychological and economic aspects of financial behavior. The study comprises information on work, pensions, housing, mortgages, income, assets, loans, health, economic and psychological concepts, and personal characteristics. The DHS data are collected from 2,000 households participating in the CentERpanel. The CentERpanel is an Internet panel that reflects the composition of the Dutch-speaking population in the Netherlands. Both the DHS as well as the CentERpanel, in which the study in conducted, are run by CentERdata.

The DHS data are made available online for all scientific researchers via the DHS Data Access system (see www.dhsdata.nl). The aim is to serve researchers worldwide by providing reliable and easily accessible data and metadata. Use of the DHS data is free of charge for scientific purposes.

In addition to using CentERdata's own (meta-) data dissemination system, the DHS data are archived in EASY, the online archiving system of the Dutch Data Archiving and Networked Services (DANS), to guarantee the long-term availability of the data. DANS is a holder of the Data Seal of Approval and one of the founding members of the Seal.

More information on the DHS can be found at:
http://www.centerdata.nl/en/survey-research/dnb-household-survey-dhs

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

1. The data producer deposits the data in a data repository with sufficient information for others to assess the quality of the data, and compliance with disciplinary and ethical norms.

Minimum Required Statement of Compliance:

3. In progress: We are in the implementation phase.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

DHS Data Access system only archives the data collected within the DNB Household Survey (DHS) and therefore does not deal with external depositors of data. DHS is one of the studies administered to the CentERpanel and owned by CentERdata. The study complies with the same data quality requirements as all studies in this panel. Information on the quality of the CentERpanel studies is publicly available at http://www.centerdata.nl/en/about-centerdata/what-we-do/data-collection/centerpanel

High quality data and scientifically sound research methods are important to CentERdata. To ensure these, CentERdata follows an internal research program. Information on this program can be found at: http://centerdata.nl/en/about-centerdata/what-we-do/research-program

CentERdata's management team governs over the data collection, archiving and dissemination of the DHS. Moreover, an external Scientific Advisory Board (SAB) oversees and advises the CentERdata management team about the DHS. The SAB advises on the design of the facility and reviews both the scientific and societal contribution of the facility. The SAB consists of CentERdata employees but also members external to CentERdata who have gained an academic expert position in the scientific fields related to the DHS.

On the DHS data website http://www.dhsdata.nl, information on the method of data collection and the construction of the datasets is provided in codebooks, which are directly accessible (without logging in) on the homepage. Additionally, a list of the   descriptives of the data variables is provided per dataset, containing information on the rate of completion of each variable. These can too be found on the homepage.

An extended review of the methodology of the CentERpanel and the DNB Household Survey can be viewed in the report 'The CentERpanel and the DNB Household Survey: Methodological Aspects', available at http://www.dnb.nl/binaries/DNB_OS_1004_BIN_WEB_tcm46-277691.pdf

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

Assessing the quality of the data looks OK, including compliance with disciplinary and ethical norms. The latter is more implicit than explicit (http://www.centerdata.nl/en/databank/centerpanel-data) stated.

2. The data producer provides the data in formats recommended by the data repository.

Minimum Required Statement of Compliance:

3. In progress: We are in the implementation phase.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

DHS data are stored and disseminated as SPSS and STATA files. The study description and variable metadata are included in documentation provided as pdf files. These are also the file formats archived in DANS-EASY. These file formats comply with the organization's file format standards for delivering panel data.

Since DHS only deals with its own data there are no formal controls to ensure compliance with these file formats. However, the file formats are checked during the internal procedure before creating an Archival Information Package (AIP). It is also part of the organization's internal Information Security and Privacy regulation to monitor changes in and guarantee support for these software packages.

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

3. The data producer provides the data together with the metadata requested by the data repository.

Minimum Required Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

The DHS project leader coordinates both the production and archival tasks of the data. The metadata production tasks therefore inherently follow their archival and dissemination requirements. As the DHS data are collected via online questionnaires, some metadata are collected and aggregated automatically during the fieldwork process. During a survey project, the DHS project leader documents the fieldwork-related metadata and creates the related documentation.

The DHS Data Access system uses Dublin Core metadata fields to describe the study. These metadata are shown on the public home page of the DHS data access website under 'DHS Description': http://www.dhsdata.nl

These Dublin Core fields are also provided for harvesting purposes at: http://dhsdata.nl/oai/. The harvesting can be done using the OAI protocol.

The system supports the main Dublin Core fields: Title, Creator, Subject, Description, Publisher, Contributor, Date, Type, Format, Identifier, Source, Language_id, Relation, Coverage, Rights.

The data which are ingested into the DHS Data Access system are also deposited in the EASY online archiving system of Data Archiving and Networked Services (DANS). Data Users have access to the metadata via the EASY system, but are referred to the DHS website to access the actual data files. The metadata fields in the EASY system follow the specifications of Qualified Dublin Core (see http://dublincore.org/documents/dcmi-terms/). Mandatory fields include: Title, Creator, Date created, Description, Access rights, Date available, Audience (the latter only in Standard).

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

4. The data repository has an explicit mission in the area of digital archiving and promulgates it.

Minimum Required Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

The DNB Household Survey (DHS) provides unique longitudinal data for the international academic community, with a focus on the psychological and economic aspects of financial behavior. The data are made available online for all scientific researchers via the DHS Data Access website (see www.dhsdata.nl). The aim is to provide reliable and easily accessible information, including data and metadata, on the DHS.

The mission and objectives of the DHS related to digital archiving are formulated by CentERdata in the Data Management and Preservation Policy of DNB Household Survey (DHS), which is available at: http://www.centerdata.nl/sites/default/files/bestanden/data_management_and_preservation_dhs.pdf

In addition to using its own (meta)data dissemination system of the DHS, the data are archived in EASY, the online archiving system of the Dutch Data Archiving and Networked Services (DANS), to guarantee the long-term availability of the data. Besides in its own system, CentERdata archives the published data files and codebooks in the EASY system of DANS. While these data files are currently accessible to Data Users via the DHS Data Access website only, CentERdata has signed a license agreement with DANS to grant access via the EASY system, in case the DHS Data Access service should ever cease to exist. This agreement is largely based on the data deposit license agreements of DANS, of which more information is available at http://www.dans.knaw.nl/en/content/dans-licence-agreement-deposited-data

Article 8 of the license agreement between CentERdata and DANS, on Dissolution of the Depositor, states the following: "In the event that the Depositor ceases to exist and there is no legal successor, datasets (or parts thereof) will be made available by the Repository as much as possible in the same access category as they were made available originally by the Depositor." While the primary goal is to guarantee long-term preservation through proper management of the DHS Data Access system, this additional measure serves to create maximum trust in long-term preservation. Furthermore, the directors of CentERdata and DANS have signed a Statement of Intent for strategic operation in data management for survey data (see http://tinyurl.com/mbbr85u).

More information on the mission and national role of DANS can be found at: http://www.dans.knaw.nl/en/content/about-dans

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

5. The data repository uses due diligence to ensure compliance with legal regulations and contracts including, when applicable, regulations governing the protection of human subjects.

Minimum Required Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

CentERdata, the owner of the DHS and the DHS Data Access system, at all times complies with applicable laws and regulations including the Dutch Personal Data Protection Act (Wet Bescherming Persoonsgegevens). Furthermore, CentERdata uses working methods that meet the guidelines developed by the Association of Universities in the Netherlands (VSNU) as set out in the Code of Conduct for the use of personal data in scientific research (VSNU, 2005).

The CentERpanel, to which the DHS study is administered, is registered with the Dutch Personal Data Protection Agency (College Bescherming Persoonsgegevens) under number m1274900. CentERdata is registered at the Tilburg Chamber of Commerce under number 41098659.

Data consumers are required to sign an agreement of usage before access rights to the data are granted. This agreement can be found at: http://www.centerdata.nl/sites/default/files/bestanden/dhs_statement.pdf

The rules and conditions for using DHS data are further described at: http://www.centerdata.nl/en/databank/dhs-data/rules-and-conditions

If a data user does not comply with the statement, the following procedure is followed:

1. The person is first personally contacted and addressed regarding the issue.

2. Case by case, we evaluate which consequences are necessary (e.g. if a third person has received the data, he needs to sign his own statement).

3. If the person does not cooperate with the found solution, we exclude the person from further use of the data (account is blocked).

4. If the consumer's manner of using DHS data appears to violate the Dutch Code of Conduct for the use of personal data in scientific research, or the Dutch Personal Data Protection Act or any other national legislation, then CentERdata may take further actions to contact the disciplinary or legal authorities, if need be."

No data which involve disclosure risks for the respondents are disseminated. All datasets are checked for personal information as part of the data quality check before publication. To further ensure anonymity, the key respondent identifier is encrypted such that it cannot be connected to the original administration ID. Furthermore, the panel management system and internal procedures maintain a strict division of roles and disclosure (e.g. panel administrators see NAW data but no survey data, researchers precisely reversed).

Within CentERdata, an officer is appointed to attend to the issue of information security/data protection and privacy. This Information Security and Privacy officer is responsible for an up-to-date knowledge level and up-to-date procedures and processes in the organization regarding these subjects. The Information Security and Privacy officer also takes part in the bi-weekly systems management meetings at CentERdata and is entitled to delegate tasks and responsibilities to system administrators and/or other officials in the organization.

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

Data security certainly looks OK. The Repository might contemplate (regular) staff training on this issue.

6. The data repository applies documented processes and procedures for managing data storage.

Minimum Required Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

CentERdata has documented its processes for managing the data storage of DHS data in a policy report, Data Management and Preservation Policy of DNB Household Survey (DHS), which is published on the CentERdata website. The processes are described based on the OAIS model in Chapter 6 of this document. This policy can be found at: http://www.centerdata.nl/sites/default/files/bestanden/data_management_and_preservation_dhs.pdf

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

7. The data repository has a plan for long-term preservation of its digital assets.

Minimum Required Statement of Compliance:

> 3. In progress: We are in the implementation phase.

Applicant Entry

Statement of Compliance:

> 4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

> In the Data Management and Preservation Policy of DNB Household Survey (DHS) (available at
> http://www.centerdata.nl/sites/default/files/bestanden/data_management_and_preservation_dhs.pdf) the DHS
> strategy for long-term preservation is formulated as follows:

> The strategy to reduce the risk of obsolescence is based on storing multiple copies on different storage media at
> different sites. If one of the sites collapses, this can be repaired by restoring the data from the other sites. To
> prevent sites from collapsing, all servers are kept in professional climate-controlled server rooms.

> Preservation ('planning functional entity') is secured further by backing up the data. All servers on which DHS
> data are stored are backed up daily. The backups are encrypted and stored at a different location. Since the data
> submitted to the DHS Data Access system is created by CentERdata, the Ingest functional entity is integrated in
> the systems of the archive. Its backup is made by VANCIS, a Dutch super-computer center.

> A System Administrator is responsible for the operational management of the server park and attends to the tasks
> of the administration functional entity. The system administrator also performs the updates of the software
> packages.

> Besides in its own system, CentERdata archives the published data files and codebooks in the EASY system of
> DANS. The metadata deposited in the EASY system are defined on study level. While these data files are currently
> accessible to Data Users via the DHS Data Access website only, CentERdata has implemented a Statement of
> Intent with DANS to grant access via the EASY system, in case the DHS Data Access service should ever cease to
> exist. While the primary goal is to guarantee long-term preservation through proper management of the DHS Data
> Access website, this additional measure serves to create maximum trust in long-term preservation.

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

8. Archiving takes place according to explicit work flows across the data life cycle.

Minimum Required Statement of Compliance:

3. In progress: We are in the implementation phase.

Applicant Entry

Statement of Compliance:

3. In progress: We are in the implementation phase.

Self-assessment statement:

The organization and workflow of the DHS from data collection to data archiving and dissemination are described in Chapters 4 and 6 of the Data Management and Preservation Policy of DNB Household Survey (DHS), available at http://www.centerdata.nl/sites/default/files/bestanden/data_management_and_preservation_dhs.pdf

The workflow of the archival ingest phase of the DHS data can be divided into two parts: ingesting the data into the DHS Data Access system, and ingesting the data into the EASY system of DANS. We describe both below.

DHS Data Access system

The DHS Project Leader is responsible for archiving the DHS data. After completing the fieldwork, the DHS Project Leader processes the data into a Submission Information Package (SIP) to be ingested by the DHS Data Access system. All data-processing steps are documented in and run using an SPSS syntax file to ensure an audit-trail to the original data file and a reconstruction of the data processing. In addition, the following protocols are being formalized and internally documented. To prepare the SIP, the Project Leader follows a procedure which is documented in the form of a checklist, containing data and metadata requirements and quality checks. For each SIP there is an internal second-reader check. Before the SIP is converted into an AIP and accepted into the DHS Data Access system, the second reader follows a Data Entry Checklist, which defines the required checks on the submitted data and metadata. In addition, the data-entry interface used to enter (meta-) data into the DHS Data Access system contains systematic checks to prevent the entry of incorrect or duplicate (meta-) data.

EASY/DANS

The data that are stored in and disseminated via the DHS Data Access system are also deposited in the EASY online archiving system of DANS. These data are systematically entered into the EASY system by the DHS Project Leader. Once these data have been uploaded to the EASY system, a designated DANS employee verifies the data and if necessary will contact the DHS Project Leader, before the data are ingested into the EASY system. For data access, the option 'Other access: no access via EASY' is used. This means that Data Users have access to

the metadata via the EASY system, but are referred to the DHS Data Access website to access the actual data files.

Each time a dataset is uploaded into the EASY system, a license agreement is digitally accepted. For more information on this license agreement, please view
http://www.dans.knaw.nl/en/content/dans-licence-agreement-deposited-data

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

9. The data repository assumes responsibility from the data producers for access and availability of the digital objects.

Minimum Required Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

Since only the data from DHS are ingested into DHS Data Access system, and both are owned and operated by CentERdata, there is no external data producer involved in the process. Actions concerning availability and crisis management of the DHS data are described below.

To ensure access and availability of its digital objects, CentERdata follows security and risk management regulations as stated in its Handbook of Information Security and Privacy. This document is based on the ISO standard NEN-ISO/IEC 27002 and is also in conformity with the Dutch 'Code of conduct for use of personal data in scientific research', published by the Association of Dutch Universities (VSNU).

All data in the DHS Data Access system are stored on servers in an especially dedicated and secured server room at Tilburg University. Only duly authorized Tilburg University server administrators and CentERdata server administrators have access to this room. To gain access to these servers, an administrator needs an electronic key and an alarm code, and must follow the procedure set out by the security officer of Tilburg University.

All data in the DHS Data Access system are stored on redundant disk servers hosted at the Tilburg University computing center. These servers are monitored with a system that sends instant messages to the system administrator on duty in case of a problem. As soon as a problem occurs, the system administrator can repair this using the redundant disk. In case of a complete system crash, or in case of a calamity affecting the Tilburg University computing center, an external backup of both the data and the system's source code are available at the Vancis datacenter in Amsterdam. Using this facility makes it possible for CentERdata to get the data access system up and running within a couple of days in case of a calamity.

Vancis BV was founded in 2008 as a subsidiary of SURFsara. Vancis offers ICT services and ICT products to enterprises, universities, and educational and health care institutions. Vancis BV takes advantage of SURFsara's know-how and experience. Both Vancis BV and SURFsara are part of SURF, the collaborative ICT organization for higher education and research in the Netherlands.

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

10. The data repository enables the users to discover and use the data and refer to them in a persistent way.

Minimum Required Statement of Compliance:

3. In progress: We are in the implementation phase.

Applicant Entry

Statement of Compliance:

3. In progress: We are in the implementation phase.

Self-assessment statement:

Access to the DHS Data Access website http://www.dhsdata.nl is easy and the study metadata are freely accessible without registration. For the quickest access, Dublin Core information fields can be viewed on the homepage under 'DHS Description'. More detailed metadata on each wave of the DHS study are included in codebooks, which are created per study wave. These are listed and directly clickable on the homepage under 'Download Codebooks'. The codebooks can be downloaded without logging in. The codebooks contain information on the study objectives, the fieldwork, the data file and the content of individual variables.

While access to metadata is unrestricted, users must register in order to download the data files. After successful registration, the data are free to every academic researcher, both in the Netherlands and abroad. The data are offered as SPSS and STATA files, which belong to the most commonly used statistical packages in the social sciences.

To enable meta-crawlers to harvest the metadata of the DHS, the system supports the OAI-PMH protocol. The metadata information based on the Dublin Core can be harvested at http://dhsdata.nl/oai/. These metadata can also be searched by Google.

To increase visibility of the DHS data, the repository can be accessed through NARCIS, http://www.narcis.nl ("The gateway to scholarly information in the Netherlands"). As the National Academic Research and Collaborations Information System, NARCIS is the main national portal for scientific information. NARCIS harvests the metadata from the DHS website using the OAI protocol.

For the future, there are plans to migrate the DHS data under a Questasy application, which is compatible with version 3 of the DDI (see http://www.centerdata.nl/en/software-solutions/questasy). This will enable deep searching of the entire database including metadata on question and variable detail level.

DANS creates persistent identifiers, in this case URNs, for the studies which are ingested by the EASY system. These can be viewed on the website of the EASY system. The persistent identifier of the DHS is also presented on the DHS Data Access website (see DHS Description).

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

11. The data repository ensures the integrity of the digital objects and the metadata.

Minimum Required Statement of Compliance:

3. In progress: We are in the implementation phase.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

In order to control the integrity of data files, MD5 and SHA1 checksums are calculated of all uploaded files (data files, codebooks, images etc.) as the file is being uploaded to the server. It is possible to check the integrity of another copy of the data file by calculating the checksum of the data file and comparing its value with the checksum which was determined during upload of the published file. For example, Data Users can use the checksum to verify the integrity of the copy of the data file which they have downloaded in comparison with the version on the DHS Data Access website. Since the checksums are currently calculated by the system but not automatically displayed externally, the Data User can do this upon request. Internally, the checksums are also used to support version management.

For each release, data files are named with file release numbers starting at 1.0. This accounts for data files (both the name of the compressed file as the data file itself), codebooks and descriptives files. When the content of a file changes, the release number of the file name changes. File names of modules change in versioning independently, thus some files of a certain module are named 1.0, others 1.2. Only the most recent version of a file is visible online / published / disseminated and available for end users to be downloaded, though every version of a file is kept archived within the DHS data access website. Only moderators can access these files. Changes that were made to files that were already published / disseminated are logged and described in a version control file on the local network of CentERdata. Within the DHS data access website, a change log file accompanies a file that has changed since its first release.

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

12. The data repository ensures the authenticity of the digital objects and the metadata.

Minimum Required Statement of Compliance:

3. In progress: We are in the implementation phase.

Applicant Entry

Statement of Compliance:

3. In progress: We are in the implementation phase.

Self-assessment statement:

In the DHS Data Access system, administrative information on database events and requests are logged and can be used to verify past events. To access the system, one must be uniquely logged in. External Data Users who are logged in gain limited rights to operate within the system, mainly to download the published datasets. Internally, CentERdata staff members also need to register to access the system. Depending on the tasks, a specific role is allocated to the staff member. The access rights within the system are dependent on this role. Each data download by both external and internal users is logged and can be traced back to the individual user. Time stamps of any changes made to data and metadata are also logged.

If the metadata or data need to be altered after ingesting the SIP into the data archive (as AIP), then the following procedure applies. The original SIP is modified by the DHS Project Leader. Before starting to process the data file, the Project Leader compares the checksums of the published version and the copy which he/she will use for the new version. The DHS Project Leader then uses the same documentation procedure as for the first version, i.e. a syntax file is used for the data file including the modifications of the data file. A new version number is allocated to the file. If the content of a data variable needs to be changed, the variable receives a new name as the interpretation of the data variable might have changed. The changes to the content are documented in the related codebook, which is saved in the internal directory of the SIP. After a check the Project Leader enters the new version of the file into the DHS Data Access system and enters information on the modifications into specified AIP fields which are visible for the Data Users. Old versions of data files remain stored in the database.

The abovementioned procedures are described in Chapter 6.4 of the Data Management and Preservation Policy of DNB Household Survey (DHS), available at
http://www.centerdata.nl/sites/default/files/bestanden/data_management_and_preservation_dhs.pdf

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

13. The technical infrastructure explicitly supports the tasks and functions described in internationally accepted archival standards like OAIS.

Minimum Required Statement of Compliance:

3. In progress: We are in the implementation phase.

Applicant Entry

Statement of Compliance:

3. In progress: We are in the implementation phase.

Self-assessment statement:

According to the OAIS model (Open Archival Information System), the data processing can be divided into six functional entities and related interfaces: ingest, data management, archival storage, access, preservation planning and administration. These different tasks are recognized by the DHS. The processes related to DHS archiving, applying the OAIS functional model, are described in the Data Management and Preservation Policy of DNB Household Survey (DHS), available at
http://www.centerdata.nl/sites/default/files/bestanden/data_management_and_preservation_dhs.pdf

Concerning future plans for infrastructure development, the DHS data are planned to be migrated under a Questasy application, which is compatible with version 3 of the DDI. CentERdata also collaborates with DANS to further develop data archiving and dissemination protocols.

For more information on DDI, visit the DDI Alliance website at http://www.ddialliance.org

For more information on Questasy, see http://www.centerdata.nl/en/software-solutions/questasy

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

14. The data consumer complies with access regulations set by the data repository.

Minimum Required Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

The use of data is free but not unrestricted. The data can be accessed only after having signed an agreement for the use of data. These agreement applications are controlled by a dedicated CentERdata employee before granting the access rights to the data consumer. The data are meant for purely scientific use only. The application procedure to obtain access rights can be viewed at: http://www.centerdata.nl/en/databank/dhs-data/rules-and-conditions

The agreement itself is available at: http://www.centerdata.nl/sites/default/files/bestanden/dhs_statement.pdf

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

15. The data consumer conforms to and agrees with any codes of conduct that are generally accepted in the relevant sector for the exchange and proper use of knowledge and information.

Minimum Required Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

CentERdata, the owner of the DHS and the DHS Data Access system, at all times complies with applicable laws and regulations, including the Dutch Personal Data Protection Act (Wet Bescherming Persoonsgegevens). CentERdata also uses working methods that meet the guidelines developed by the Association of Universities in the Netherlands (VSNU) as set out in the Code of Conduct for the use of personal data in scientific research (VSNU, 2005). This Code of Conduct is available at (in Dutch): http://www.vsnu.nl/files/documenten/Domeinen/Accountability/Codes/Bijlage%20Gedragscode%20persoonsgegevens.pdf

The DHS data consumer is also expected to follow the abovementioned laws and guidelines where applicable. Specifically, the DHS data consumer agrees to conform to the following codes of conduct, which are customary for using data in social sciences and are stated in the DHS data usage agreement:

1. He/she undertakes to keep confidential any information in the CentER Savings Survey and DNB Household Survey concerning individual persons, households, enterprises or institutions which comes to his/her knowledge during the work on these projects.
2. He/she undertakes not to distribute data of the CentER Savings Survey and DNB Household Survey to others without permission from CentERdata.
3. He/she undertakes to use the data for purely scientific (i.e. non-commercial) research only.
4. This statement shall remain valid, even after conclusion of the work specified.

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

16. The data consumer respects the applicable licences of the data repository regarding the use of the data.

Minimum Required Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

The data consumer signs the 'Statement Concerning the Use Of CSS & DHS Data' and thereby undertakes to comply with its regulations (see at http://www.centerdata.nl/sites/default/files/bestanden/dhs_statement.pdf). If the data consumer does not comply with the regulations as stated in the data usage agreement, then his/her access rights to the further use of data can be withdrawn by CentERdata as the data are only available via a password-protected login onto the DHS Data Access system. If the consumer's manner of DHS data usage appears to violate the Dutch Code of Conduct for the use of personal data in scientific research, or the Dutch Personal Data Protection Act or any other national legislation, then CentERdata may contact the data consumer regarding the issue. If need be, CentERdata may take further actions to contact the disciplinary or legal authorities.

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments: