ANNEX 19: CODE OF PRACTICE FOR THE SECONDARY USE OF MOBILE NETWORK BIG DATA

;

;

IDRC Grant/ Subvention du CRDI: 108008-001-Leveraging Mobile Network Big Data for Developmental Policy

Annex 20: Code of Practice for the Secondary Use of Mobile Network Big Data

Definition of terms

AGGREGATED DATA	Data of several individuals that have been combined to show general trends or values.
ANONYMISATION*	Process of removing all elements allowing the identification of an individual person (i.e., of rendering data anonymous).
ANONYMISED DATA	Data which was identifiable when collected but which are not identifiable anymore (have been rendered anonymous). Anonymous data are no longer personal data.
DATA CONTROLLER (or Controller)*	The natural or legal person, or any other body, which alone or jointly with others determines the purposes and means of the processing of personal data
DATA PROCESSOR (or Processor)*	The natural or legal person, or any other body, which processes personal data on behalf of the controller.
DATA SUBJECT	The person whose personal data are collected, held or processed.
DE-IDENTIFICATION	Process of rendering data pseudonymised or or annonymised
PERSONAL DATA*	Any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
PROCESSING	Any operation or set of operations which is performed upon personal data, whether or not by automatic means such as collection, recording, organisation, storage, adaption or alteration, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
PSEUDONYMISATION	Process of removing all elements allowing the identification of an

	individual person, except the key(s) allowing linking the data to the person. Such key shall be randomly generated and subject to technical and organisational measures to prevent its unauthorised use
PSEUDONYMISED DATA	Personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution. The only difference between pseudonymised and anonymised data is that in the latter case there exists no key to link data to the data subject
RE-IDENTIFICATION	The process of linking de-identified data to the study participant.
SECONDARY USE OF DATA (or Data Re-Use)	Processing of already existing data for a purpose different from the purpose for which they have been initially collected
THIRD PARTY*	Any natural or legal person other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data.

ARTICLE 1 – General Provisions

1. SCOPE

This Code will address issues related to the processing and use MNBD**.**

2. ADHERENCE

Where applicable, adherence to this Code of Practice (hereafter Code) can be effective by reference to it in a legally binding document, contract or unilateral declaration (see Appendix 1).

This Code strictly aims at facilitating compliance with applicable legislation.

The term "shall" in this Code means the action is obligatory.

ARTICLE 2 - Collection, of Mobile Network Big Data (MNBD)

RULE 1: The Data Controller shall ensure that:

- The data collection complied with the applicable legal and ethical requirements, and;
- [to the extent feasible], data collection practices will be transparent and will not go beyond /will desist from collecting more data than needed for the efficient operation of the network and the supply of goods and services to the customer.

ARTICLE 3 – Use of Mobile Network Big Data (MNBD)

RULE 2: All users and related uses of MNBD must provide for appropriate technical and organizational measures that protect personal data against accidental destruction or loss, alteration and unauthorized disclosure or access. This includes**:**

- The development and enforcement of a policy to ensure the confidentiality, protection and security of data, including documented training on the policy.
- Computerised systems which are access controlled and protected against physical and electronic intrusion, and,
- Technical security measures complying with the relevant guidance and regulations as applicable.

Secondary use of data

RULE 1: The secondary use and/or transfer of data will be subject to this Code and relevant/ current legal and ethical requirements.

RULE 2: The secondary use of data shall be limited to anonymised data.

RULE 3: All parties involved in the transfer and use of secondary data shall identify risks and make best efforts to prevent the de-anonymisation of data. This includes through processes that provide for the regular monitoring of techniques related to the anonymization and de-anonymisation of data.

Individually identifiable data/Personal data

RULE 4: The Data Controller shall not release individually identifiable data to third parties UNLESS:

- Specific consent has been obtained from the individual(s).
- The data use/purposes are specified and have been approved by an ethics committee set up or this purpose. (Process of setting up ethics committee??)
- If an ethics committee is not available, approval from an equivalent third party review is required.

RULE 5: The transfer of individually identifiable data /personal data to third parties shall require that the maintenance of the protection of individually identifiable data/Personal Data is guaranteed by the recipient.

RULE 6: The transfer of identifiable data by the data controller to a third party shall be subject to the following requirements:

- Transfers responsibility from the data controller to the third party to maintain safeguards to ensure security of individually identifiable data.
- Requires the third party to identify and minimise any risks associated with the release of this data to the third party consequent to the increased accessibility of this data.
- The third party to be aware of and the Data Controller to provide all relevant information on any restriction of use or obligation applicable to the data if any (e.g., the limited scope of purposes imposed by the consent form, limitations related to providing data to third parties, the obligation to report incidental findings, etc.).

Non -discrimination

RULE 7: The principle of non-discrimination shall govern the release of all MNBD to third parties who do not compete with the relevant MNO.

RULE 8: All parties in the same class shall be treated equally, subject to resource constraints

ARTICLE 4 – De-identification and Protection of Anonymised Data

RULE 9: In order to pseudonymise or anonymise personal data, state of the art deidentification measures have to be taken to remove and/or to conceal sufficient direct and/or indirect identifiers (see Appendix 3). The number and the selection of identifiers to be removed, depends on the risk for privacy violations. The data controller shall document the de-identification methods applied and ensure that the identifying key is securely stored (or destroyed in case of anonymisation).

RULE 10: De-identification of data shall only be done by persons authorised to have access to the data and bound to confidentiality.

RULE 11: Personal Data which have been pseudonymised shall not be considered personal data in the hands of a user who does not have access to the key if:

- The de-identification process is compliant with this Code, and,
- A binding agreement defines the conditions under which the data can be used, and,
- Appropriate technical measures have been taken to minimize risk of reidentification, as set out in Article 3.

RULE 12: Aggregated data are considered anonymous data provided safeguards are taken to avoid the risk of re-identification of data subject to the provisions of the Code (e.g. Article 3).

ARTICLE 5 - Documentation and Data Retention

RULE 13: Any secondary use or sharing of data with third parties shall be documented.

RULE 14: Retention periods should be defined and retention period shall be communicated to any third party to whom the data shall be transmitted.

RULE 15: Pseudonymised research data may be stored on the computer systems of the member organisations or of their authorised partners/ processors/ third-parties, as long as it may be required for further lawful research, subject to on-going appropriate technical and organisational safeguards.

RULE 16: Anonymous research data may be stored as long as necessary.

ARTICLE 6 – Data Disclosure

RULE 17: Pseudonymised data shall not be publicly disclosed.

RULE 18: Anonymised data disclosure shall follow state of the art de-identification methods (see Appendix 3) according to the following principles:

- De-identification is performed in a way that reduces the risk of the data being associated with an individual, and,
- - Where data is disclosed to third parties, these parties are subject to an agreement (available on-line/provided by data controller without a charge??) which will include requirements that:
    - prohibits any attempts to re-identify subjects and to share these data with other third parties,
    - provides for appropriate state of the art data security measures are taken, including control and monitoring of data downloads,
    - ensures the risk of potential re-identification of the data remain limited within reasonable means, and;
    - subject to requirements under Article 3 rule 6

RULE 19: Accountability for maintaining disclosed data anonymous (i.e., not re-identifiable) shall be clearly assumed by the relevant data controller(s). In the event that the risk of re-identification becomes unacceptable, the controller(s) should deny and/or revoke access to such data.

ARTICLE 7 - Implementation of the Code Rules

RULE 20: Each entity processing and using MNBD should:

- Establish internal procedures to transpose personal data protection rules into binding requirements or to make this Code (see Appendix 1) binding,
- Where necessary, anticipate and define specific rules (e.g., sanctions), and;
- Ensure that the procedures are implemented and easily accessible to all persons having access to MNBD.

ARTICLE 8 - Code modifications

This Code of Practice will be reviewed and revised periodically by a panel of MNO's, data protection and ethics experts to ensure continued compliance with relevant national and international regulations. This periodic review will be organized by xxx

Each version of the Code will be clearly labelled and referred to with a Code version number, the date of publication and a summary of the substantial changes.

APPENDICES

Appendix 1: Adherence Agreement (given as an example to render this Code binding)

Mr. / Ms. [First Name, Last Name],

Acting on behalf of [Firm / legal entity], holding the position of [position] herewith declares:

- I have the legal capacity to represent and engage [Firm/legal entity] for the purpose of this project.
- [Firm] agrees to fully endorse and adhere to the [Code full name], Version [Version] of [date]. It shall apply to all data processing activities carried out within the project [Project name]. The personal data protection framework is thus in part formalized through this Code.
- [Firm] will ensure the implementation of all measures required by the provisions of this Code.
- [Firm] will ensure compliance with this Code by all staff and personnel working within the project on behalf of [Firm].

In addition to the rules laid out by the [Code], the following project specific rules shall apply:

- [To be developed as needed for each project/purpose]

Signed on behalf of [Firm name] on [Date] by [print name]: _____

Appendix 2: Examples of de-identification methods and guidance

The risk for re-identification is dynamic and may change as technology improves and costs decrease. The following criteria may help to define which de-identification and security measures shall be taken:

• How many people have access to the data?
• Are these people bound to confidentiality?
• How high is the interest in re-identification?
• What is the level of the organizational and technical protection measures?
• How long will the data be stored?
• Will the data set be enriched over time?

This also requires balancing the four following parameters:

• level of de-identification
• motives and capacity to re-identify
• risk of invasion of privacy (potential impact on person’s privacy)
• level of controls/ security measures in place.