

DOI: <https://doi.org/10.71447/3005-2696-2026-01-04>

DATA PRIVACY OF AGRICULTURAL HOLDERS IN THE 2024 AGRICULTURE CENSUS OF IRAN

Seyyed Mahdi Sadati Nooshabadi

Statistical Centre of Iran

Expert on International Affairs and Statistics

Tehran, Iran

E-mail: mnooshabadi2009@gmail.com

Abstract

Data privacy of respondents and confidentiality of statistics are integral parts of the surveys that the National Statistical Offices conduct. These elements ensure the respondents of the confidentiality of the data they provide and how these data are used to benefit the society. The National Statistical Offices employ different strategies to increase the participation rate in their surveys which contribute to the quality and confidentiality of the collected data. The Statistical Centre of Iran, which is considered the sole provider of official statistics on the socio-economic situation in Iran, conducted the last National Agriculture Census of Iran in the Autumn of 2024. This paper looks at the adopted provisions of this Centre for preserving the confidentiality of the data of agricultural holders aimed at avoiding the data leak and preserving the data privacy and confidentiality of statistics they provided. The Statistical Centre of Iran practiced the protocols of the Information Security and Management System (ISMS) as the management system for its data privacy and also follows its own Data Confidentiality Assurance Policy. The objectives of this system and policy were to ensure the protection of the information assets of the Statistical Center of Iran such as the data and information obtained from censuses, sampling methods, and administrative and statistical records that are stored in the servers, workstations, and its databases. The activities done based on these provisions and procedures in this census including the training of the individuals working in all the fields of the census on the issue of confidentiality of statistics and how to preserve it, regularly delivering of all the concerned documents such as filled questionnaires and other hardcopies of information to the supervisors, restricting the individuals who can access the filled questionnaires and determining authorized people for accessing the data inputting sites led to securing the privacy of collected data and ensuring the agricultural holders of the confidentiality of their statistics.

Keywords: Data Privacy, Statistical Confidentiality, Agriculture Census, Information Security and Management System

INTRODUCTION

The National Statistical Offices (NSOs) of countries employ various strategies, principles and practices to respect and protect the data privacy and confidentiality of statistics provided by respondents in the surveys. The NSOs usually publish the ultimate goals of conducting their surveys and inform the respondents about the survey's purposes. This transparency helps the respondents to make informed decision and provide accurate data. Ensuring the respondents about the confidentiality of their data contributes directly to the quality of the collected data. The respondents must be confident that their data are solely used for statistical purposes in order to provide true and accurate data.

The Statistical Centre of Iran (SCI) follows a set of rules, guidelines and procedures to preserve the data privacy and ensure public about the confidentiality of its collected statistics. These rules are obligatory and all the activities related to the surveys and statistical activities of the SCI are designed and conducted by following these rules. The article seven of the Law of the SCI puts a roadmap for preserving the data privacy of the respondents. This article implies that all the data collected and obtained from the individuals or organizations during conducting the surveys are confidential and may only be used for production of general statistical information.

The SCI follows the international recommendations for conducting surveys such as the fundamental principles of official statistics and also practices a practical approach for preserving the confidentiality of statistics in line with its Information Security Management System (ISMS). The domain of this management system is all the data resources, organizations, and third parties which have connection with or use the data and statistics owned by the SCI. This system explains how the collected data should be handled and what are the responsibilities of each person for preserving the confidentiality of statistics.

Moreover, one of the core institutional values of the SCI is the trust worthiness and confidentiality in personal information. According to this value, the SCI takes all the necessary considerations and needed legal obligations for collecting, processing, and disseminating of statistical information. The statistical dissemination policy of the SCI also reflects its professional loyalty to the issue of data privacy. According to this policy, the SCI ensures that the statistical information does not disclose any information about the statistical unit such as name and business ID number. The users can access to microdata only after deletion of any identification factors of the statistical units. The confidentiality of statistics is also presented in the data security document of the SCI. This document informs the users and respondents about how their data and statistics are used and explain the mission of the SCI to protect the confidentiality of the collected statistics.

This paper is going to explain the procedures taken in the 2024 Agriculture Census of Iran to protect the data privacy of the agricultural holders based on its ISMS and data policy. Moreover, this paper looks at the provisions and procedures which the SCI adopted for preserving the confidentiality of the data of agricultural holders, avoiding the data leak, and preserving the confidentiality of statistics while inputting the data. The activities done based on these provisions and procedures such as training of the

individuals on the importance of confidentiality of statistics and data privacy, delivering of the concerned documents to the supervisors, setting up restriction on access to the filled questionnaires and data imputing sites contributed a lot to securing the privacy of collected data and ensuring the agricultural holders of the confidentiality of their statistics.

In the second section of this paper, the legal aspects of data privacy in Iran are explained and then the practice of data privacy in the SCI realized by its Information Security and Management System and Data Confidentiality Assurance Policy are described. In the last part, the practice of data privacy in 2024 Agriculture Census of Iran is described and the taken procedures and provisions are discussed.

Legislation on confidentiality and data privacy in Iran

Data privacy and confidentiality of statistics in surveys are important areas of researches due to the growing concerns surrounding personal data protection and the implications of data sharing. A review of the employed strategies and practices of organizations such as the European bureau of statistics (EUROSTAT) and the UNECE¹ for conducting surveys shows that the most used methods for preserving the data privacy of respondents are informing the participants about the mandatory or voluntary participation in the survey and the nature of questions, designing and using of clear and concise questions and anonymizing the data and removing of any identity revealing elements from the provided answers.

A review of data policy law across the countries shows that many countries have established the necessary laws and regulations aimed at protecting the privacy and security of data received from the people. The European Union adopted the GDPR² which emphasizes the issues such as obtaining user content, data minimization and the right to be forgotten³. In Africa, The African Union Convention on Cyber Security and Personal Data protection tries to harmonize the efforts of African countries on data protection laws. Other countries are practicing more or less the same. For example, the USA employs laws like HIPAA⁴ for health data and the COPPA⁵ for children's data. China has approved the law named PIPL⁶ to regulate how data should be collected, stored and shred. Brazil has established a law similar to GDPR in order to protect the user rights and principles concerned with data protection. The Privacy Act 1988 in Australia regulates issues related to data privacy.

There is no comprehensive data protection legislation in Iran but several laws and regulations provide data protection provisions. Sharia law, derived from Islamic teachings, provides guidance on various aspects of life, including the protection of personal data. The results of researches by various researchers such as Al Khatib (2018), Abdul Aziz (2019), and Al Muqrin (2020) concluded that Sharia Law puts

¹ United Nations Economic Commission for Europe

² . General Data Protection Regulation

³ . <https://gdprlocal.com/data-protection-laws-around-the-world-a-global-perspective/>

⁴ . Health Insurance Portability and Accountability Act

⁵ . Children's Online Privacy Protection Act

⁶ . The Personal Information Protection Law

emphasis on data policy by taking into consideration the crucial issues such as confidentiality, necessity, consent, purpose and access. It is obligatory to take consents of the people for disclosing of their personal data and limiting the usage of provided data just for the specific purposes for which the data has been collected. The Constitution of the I.R. Iran in the Articles 22, 23, and 25 which are about the rights of nation, defines the domain of the personal privacy of people in terms of dignity, life, housing, beliefs, letters, phone calls and electronic communications. Based on the article 38 of the Islamic Republic of Iran Charter on Citizens' Rights (December 2016) "Collection and publication of private information of citizens is forbidden, except with their informed consent or pursuant to the law". Cyber Crime Act (2011) has determined punishment against whom accused of disclosing or destroying the data in order to disturb public order or other people (Articles 16 to 18). According to this law (Note 2, Article 32) the user information includes the information on identity, mailing address, IP address, telephone number and other personal information (private photo and films). Based on the Law on Dissemination of and Free Access to Information, which was enacted in 7 July 2009, the personal information are name, surname, home and work address, the situation of family life, personal habits, physical problems, bank account number, and passwords. Based on the Article 14 of this law, any request to personal information is considered as violation of privacy. Based on the article 65 of the Electronic Commerce Law (ECL 2004), the data of people and companies which has economic value such as financial data, trade plans and list of customers which are not available to public are considered as trade secrets and illegal access to this information is banned by this Law. According to the article 27 of Bylaw Concerning Official Translators 1996, the translator is responsible to maintain the privacy of the customer information which he becomes aware of it due to translation process. The government of Iran in 2023 approved an instruction on protecting the people's data which concerns with the protection and data privacy of people. According to this instruction, the executive agencies are obliged to do specific activities in line with data protection. For example, the ISP are to encrypt the data received from the users. According to article 729 of the Islamic Penal Code (Amended in 2024), anyone who illegally accesses data that are protected by security measures is subject to be imprisoned. According to the article 232 of Iran Direct Tax Law, the financial information of people obtained during the tax determination process are considered confidential and must not be used or disclosed for any purpose except assessing income and taxes.

Practice of Data Privacy in the SCI

The article seven of the Law of the SCI puts a roadmap for preserving the data privacy of the respondents. This article implies that all the data collected and obtained from the individuals or organizations during conducting the surveys are confidential and may only be used for production of general statistical information.

One of the missions of the SCI is respecting confidentiality of the personal information. In this regard, the SCI has prepared four National Strategies for Development of Statistics in Iran in which the issue of confidentiality of statistics plays an important

role. One major part of the executive policies of these strategies is paying special attention to confidentiality of individual information which are collected while conducting the surveys. This policy is in line with the sixth principle of the fundamental principles of the official statistics.

The SCI practices the protocols of the ISMS as the management system for its data privacy. The objective of this document is to protect the data assets of the SCI obtained from censuses, sampling methods, and administrative and statistical records that are stored in its servers, workstations, and databases. Protecting this data and information against all internal, external, intentional or accidental threats is another goal of this document. This document is also in line with all national laws and international recommendations, especially in compliance with the Law of the SCI, article seven of the Fifth Development Plan of the country, the National Statistical Development Program in the field of information confidentiality, and the Quality Framework of the Statistics of the SCI. The ISMS has been thoroughly and properly prepared and formulated, and it is mandatory for all stakeholders to follow it.

Based on this policy for preserving the confidentiality of statistics, the SCI prepared its vision document and intended to be the sole reference of the statistical system of Iran, trusted by the general public and professionals. The SCI has the mission of contributing to preparation and dissemination of official statistics of country and establishing a statistical system based on the observance of fundamental principles of official statistics. This Center is committed to preparing up-to-date, timely, and reliable statistics based on scientific and statistical methods and within the framework of the quality management of the official statistics system of Iran, in a cost-effective manner, and providing them to users while observing the principle of data confidentiality.

The SCI protects the information obtained from censuses, sampling surveys, and administrative and statistical records as the most valuable sources of information in Iran's statistical system to provide statistical services to users. The identification, monitoring, evaluation, and management of risks related to information security are also part of the SCI's responsibilities, based on the criteria of data and statistical information confidentiality. The strategic plan of the quality management system of statistics at the SCI provides the groundwork for the identification, monitoring, evaluation, and management of data and statistical information confidentiality. This document has been approved by the Strategic Committee on Information Security of the SCI and will be reviewed annually or when there are changes in quality requirements. Based on this policy, the data and statistical information of individuals are protected to ensure that no identification of statistical unit is possible. Public statistics are made available to everyone according to the relevant laws and regulations. In line with this goal, the SCI complies with legal, statutory, and contractual requirements outlined in the Law of the SCI, the Law on "Publication and Free Access to Information," and other government approvals and contractual obligations with third parties in the field of data provision and utilization, and statistical information is ensured. Moreover, the staff members of the SCI are trained about the confidentiality of data and statistical information.

The information security manager, on behalf of the Head of the SCI, is responsible for creating, implementing, monitoring, reviewing, maintaining, and improving the

effectiveness of this policy and its related executive procedures.

Data Privacy in 2024 Agriculture Census of Iran

The SCI follows an executive procedure for data and statistical information confidentiality to realize its ISMS. This procedure defines and sets all the principles necessary for ensuring the confidentiality of data and statistical information as stipulated in the articles 7 and 9 of the Law of the SCI, principle 6 of the Quality Management Framework for Official Statistics, and the Ten Fundamental Principles of Official Statistics of the United Nations. All the data resources, staff members of the SCI, organizations, and third-party contractors who interact with the data and statistical information of the SCI are subject to this procedure.

This procedure provides clear definition for all the crucial entities such as statistical unit (Annex One). According to this procedure, the hierarchy of operations for ensuring the confidentiality of data and statistical information are: information security strategic council, data trustees, deputy of information technology and communications section, security office, and thematic offices.

The Information Security Strategic Council is responsible to decide on the publicity of the information. This council decides on which information can be published as public microdata files.

The Data Trustees include the heads of thematic offices, the head of the Statistical Methodologies and Sampling surveys, Office of Standards, Supervision and assessment of Statistical Surveys, and Information and Communication technologies, and Cyber Security Centre. The responsibilities of these trustees include uploading necessary files to the secure environment, removing data files and sample files from the secure environment after obtaining approval from the relevant thematic office head and informing the Security Office of file removals by completing the relevant form. It should be noted that only the responsible author from the Information and Communication Technologies, and Cyber Security Centre is authorized to remove public microdata files, non-publishing tables, and applications from the secure environment after obtaining approval from the relevant thematic office head.

The Information and Communication Technologies, and Cyber Security Centre is responsible for preparing technical specifications for data files, uploading data files, creating public and licensed microdata files for user access, following the guidelines of the thematic offices, applying user access levels to licensed microdata files, following the guidelines of the thematic offices, managing access to data files and applying disclosure control methods to data files and statistical tables after receiving instructions from the thematic offices.

It is worthy to say that if any authorized changes are made to the final version of data files or statistical information, disclosure control procedures must be reapplied. The encryption of identification keys in data files and the maintenance of decryption files are the responsibility of the Information and Communication Technologies, and Cyber Security Centre. The thematic offices determine the effective identification keys. Moreover, user access to files is granted only after completing the relevant access form and signing a non-disclosure agreement.

The Security Office is responsible for physically receiving data files from executive bodies, storing received files in the secure environment, managing the storage and archiving of files received from executive bodies, in accordance with the Information Security Management System, verifying the eligibility of users requesting licensed microdata files, monitoring all transactions related to licensed microdata files in the secure environment and data workshops, managing and controlling access to the data workshop.

Each thematic office is responsible for preparing guidelines for creating public and licensed microdata files for user access, preparing guidelines and determining user access levels to licensed microdata files, preparing guidelines and rules for applying disclosure control to data files and statistical tables, determining effective identification keys and informing the Information Technology and Communications Deputy for encryption purposes.

As a general consideration, the public microdata files are made available to the public free of charge or for a fee, in accordance with the government approved tariff for statistical services. Center employees are also subject to this rule if they require the files for personal use.

Licensed microdata files are made available to users only after applying disclosure control methods, verifying user identity, and obtaining approval from the Information Security Strategic Council. Users must sign a non-disclosure agreement, too.

Framework and sample household files must not be provided to individuals or legal entities, except for thematic offices, statistical supervision offices, and provincial planning and management offices for the execution of statistical surveys. Framework files are provided to users only with information fields such as name, address, and activity code. Sample framework files are not provided to individuals or legal entities, except for thematic offices, Standards, Supervision and assessment of Statistical Surveys office, and provincial planning and management offices for the execution of surveys.

To develop and enhance information systems of executive bodies for statistical purposes, the IT Center may provide microdata to the respective bodies after verifying their data production processes and signing a bilateral agreement. The content of the agreement must comply with this procedure.

The SCI has conducted the national agriculture census in Iran in the years 1973, 1988, 1993, 2003 and 2014 in order to provide statistical framework needed for conducting sample surveys set to be implemented between censuses. These censuses also helped to collect data on structure of agriculture statistics. The 2014 agriculture census in Iran took place from 27 September to 9 November 2014 and the Ministry of the Jihad-e-Agriculture cooperated with the SCI to implement this last round of agriculture census. The method used for collecting data in the 2014 agriculture census was face-to-face interview with the agricultural holders. The enumerators used tablets to collect the needed data which were information of agricultural holders (such as name, age, national ID number and address), literacy status, land use and production details and the greenhouse activity. These agriculture censuses have provided valuable data on number and characteristics of agricultural holders, land use, agricultural land area (land area under temporary crops, fallows, and permanent crops), production of

temporary and permanent crops, number of small live stock (sheep and goat) and large livestock (cattle, buffalos and camels), milk production by type of livestock, greenhouse production, using agriculture machineries and equipment in holdings, area under modern irrigation system (sprinkle and drip system), raising poultry via traditional method, apiculture (number of hives with colonies and honey production) and sericulture (number of egg box and production of cocoon). The statistical population of the agriculture censuses were all agricultural holdings in rural and urban areas.

The 2024 round of Agriculture Census in Iran took place between 2 November – 19 December 2024. This national level statistical activity was based on the following criteria:

- Agricultural holding has been the primary statistical unit, while agricultural operator and village/city are the other two used statistical units.
- Information collection was based on referring to the agriculture holders and completing the questionnaire according to their statements. In cases where accessing the agriculture holders was not possible, other informed individuals connected to the agriculture holders were consulted.
- Lists of agriculture holders in most rural areas and cities were prepared through house-to-house visits. For 367 cities and 633 villages, administrative/registry sources, local informants, and field research methods were used to compile these lists prior to the census.
- After data collection and data entry into tablets, the information underwent multiple review stages by responsible experts, technical/educational deputies, and senior specialists. Corrections were made based on available evidence or by re-contacting operators, following technical guidelines.

The 2024 National Agricultural Census in Iran was the second large-scale survey in the country, transitioning from a paper-based to a fully electronic data collection method. Data was recorded via web-based electronic questionnaires or tablet devices. This shift in data collecting has significantly reduced costs associated with paper purchases, form printing, document storage, and eliminated certain organizational roles (e.g., review tiers, group supervisors) and census processing roles (e.g., data entry clerks, verification operators, subject-matter editors) compared to past censuses.

The data collection software was designed to enable real-time data validation checks during form completion by census enumerators through intelligent software tools. The custom

web-based software allowed technical/executive responsible experts, technical/educational deputies, and senior specialists to monitor the performance of their subordinate teams using personal smartphones or computers. They could identify, correct, or return flawed data to lower tiers for revision.

In this census, pre-census lists of agricultural operators were prepared for pilot cities and large villages. The costly and time-consuming location-by-location household listing method (to identify agricultural households) was eliminated. Instead, operator lists were compiled using registry sources and local informants before the census. Data was then collected via web-based forms and telephone interviews.

Comparative analysis of data from the 2014 census and the current enumerators'

records was enabled through management dashboards. These dashboards, developed in collaboration with the Census Secretariat, Planning and Training Committee, and IT Committee, played a key role in improving coverage, data quality, and real-time monitoring of fieldwork progress.

Tablet devices were removed from technical/executive experts, deputies, and senior specialists. Instead, mobile phones and web-based computers were used to supervise enumerators, marking another innovation in this census.

The issues of data privacy and confidentiality of the statistics provided by the respondents have been of great importance in all of the activities of the SCI. Based on the provisions and procedures of the ISMS, the individuals working in all the fields of the census should be trained on the issue of confidentiality of statistics and how to preserve it. Moreover, all the concerned documents such as filled questionnaires and other hardcopies of information to the supervisors must be regularly delivered to the concerned authors. This activity is aimed at restricting the individuals who can access the filled questionnaires and determining authorized people for accessing the data inputting sites which led to securing the privacy of collected data and ensuring the agricultural holders of the confidentiality of their statistics. All of these activities are in line with Legal Foundations of Data Confidentiality such as the Article 7 of the Statistical Center of Iran Act which stipulates that individual farmers' information, including name, surname, address, and specific details, shall remain confidential and shall not be shared with any judicial, administrative, or tax authorities. Census results are published only in aggregate and general formats.

The SCI also used Technical Methods for Data Confidentiality. These methods were the Encryption Techniques (symmetric and asymmetric encryption methods) to ensure the security of collected data. In the 2024 census, tablets equipped with secure software were used to record information. This approach significantly reduces the risk of data leakage compared to previous paper-based censuses.

The SCI considered the Operational Safeguard activities in order to preserve the data privacy of the respondents too. These activities included Restricted Access to Data in a way that only trained experts with special authorization have access to raw data. These individuals undergo security training to prevent unauthorized disclosures. Additionally, the Regulatory Bodies monitored the data collection and processing processes.

There was also Penalties for Data Disclosure. The unauthorized publication of census details (such as farmers' names and addresses) is considered a criminal offense and is subject to legal prosecution. Maintaining data confidentiality enhances farmers' participation in future censuses, as they are reassured that their information will not be misused.

CONCLUSION

This paper studied the methods and approaches towards keeping data privacy of respondents in the 2024 National Agriculture Census in Iran. Based on the existing legal frameworks and the Law of the SCI and also its ISMS provisions, the SCI practiced the provisions and protocols to preserve the data privacy of agriculture holders via

methods such as the training of the individuals working in all the fields of the census on the issue of confidentiality of statistics and how to preserve it, regularly delivering of all the concerned documents such as filled questionnaires and other hardcopies of information to the supervisors, restricting the individuals who can access the filled questionnaires and determining authorized people for accessing the data inputting sites. This strategy paved the way to ensure the agricultural holders about the issue of keeping their data safe.

Annex One: Concepts and definitions used in the executive procedure

Center : Refers to the Statistical Center of Iran.

Confidentiality : The protection of data or information related to any statistical unit against unauthorized disclosure, as defined by relevant laws and regulations.

Statistical Unit : Any member of the target population.

Statistical Information : Any product of the statistical system, including microdata, metadata, tables, charts, reports, analyses, definitions, concepts, statistical maps, etc.

Statistical Table : A table containing aggregated data of statistical units.

Microdata : Data at the level of a statistical unit or object.

Metadata : Any explanation or description of the data in question.

Paradata : Metadata specifically generated during data collection and processing.

Statistical Data : Data produced during the routine operations of an executive body.

Data File : A file containing microdata, metadata, or a combination thereof. In the Information Security Management System, this file has a standard and unique name, with version number and date included in the file naming convention.

Initial File : A file containing data from questionnaires or administrative records, uploaded by field operators during the execution of statistical surveys.

Raw File : A file containing data that has undergone initial processing by field operators but is not editable by them.

Processed File : A file that has undergone further processing and cleaning by the Center.

Final File : A processed file that has undergone anonymization and disclosure control, ready for the extraction of final tables.

Public Microdata File : A file containing microdata prepared in a way that minimizes the risk of identifying statistical units. This file is made available to the public.

Licensed Microdata File : A file containing microdata, prepared in accordance with this procedure, and made available to authorized users for research purposes. This file is not publicly available.

Framework File : A file containing the sampling framework for statistical surveys.

Sample File : A file containing sampled units selected from the sampling framework.

Decryption File : A file containing codes assigned to anonymized microdata records and some metadata removed from the microdata file.

Disclosure Control : A set of methods used in data driven research to ensure that no individual, workshop, or organization can be identified from published tables or results of statistical analysis.

Anonymization : The process of removing or altering information that could identify

individuals or entities.

Secure Environment : An environment where all principles of the Information Security Management System (ISMS) are implemented, ensuring the availability, integrity, and confidentiality of the content.

Data Workshop : A secure facility within the Center where licensed microdata files can be accessed by external users under strict security protocols.

Users : All individuals who use data and statistical information provided by the Center, including natural and legal persons, public and private sectors, national and international entities. Employees of the Center are also included in this definition.

Data Producer :

Within the Center : Any thematic office that collects data through statistical surveys or national calculations.

Outside the Center : Any executive body or public/private institution that collects data through administrative processes or surveys related to its organizational mission.

Information Security Management System (ISMS) : A system based on the PDCA (Plan Do Check Act) cycle, designed to ensure continuous improvement in information security within the organization.

REFERENCES

1. Abdul Aziz, M. (2019). Data Protection in Islamic Law. *Journal of Islamic Studies*, 30(3), 391 418.
2. Al Khatib, A. (2018). Personal Data Protection in Sharia Law. *International Journal of Law and Technology*, 5(1), 1 17.
3. Al Muqrin, M. (2020). Ethical Implications of Data Protection in Islamic Law. *Journal of Information, Law and Technology*, 25(1), 1 22.
4. <https://www.ncbi.nlm.nih.gov/books/NBK447395/>
5. <https://projecteuclid.org/journals/statistics-surveys/volume-5/issue-none/Data-confidentiality-A-review-of-methods-for-statistical-disclosure/10.1214/11-SS074.pdf>
6. <https://www.enzuzo.com/blog/data-privacy-statistics>
7. <https://unece.org/DAM/stats/publications/Managing-statistical-confidentiality-and-microdata.access.pdf>
8. <https://teo.site.ined.fr/en/survey-respondents/data-privacy/>
9. <https://ec.europa.eu/eurostat/web/microdata/statistical-confidentiality-and-personal-data-protection>
10. <https://www.sciencedirect.com/science/article/abs/pii/S0169716116300190>
11. https://www.researchgate.net/publication/292304502_A_Statistical_Approach_to_Provide_Individualized_Privacy_for_Surveys
12. <https://microdata.fao.org/index.php/catalog/1628>
13. https://amar.org.ir/en/News/ID/3518/Implementation_of_the_Fourth_Iranian_National_Census_of_Agriculture