27/2013. HCSO Regulation
on Data Protection

In order to ensure the protection of statistical data during data processing – in accordance with Regulation 223/2009/EC on European statistics, the Act No. CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information, and the Act. No. CLV of 2016 on Official Statistics as well as the Confidentiality Policy of the Hungarian Central Statistical Office (hereinafter referred to as: HCSO) – I hereby issue the following regulation.

1. §
Purpose of the Regulation

The purpose of this Regulation is to implement the Confidentiality Policy of the HCSO and to provide a common regulative framework for the data protection activities.

2. §
Scope of the Regulation

(1) The personal scope of the Regulation relates to all public service officers, public service administrators and employees (hereinafter referred to as: employees).
(2) The material scope of the Regulation relates to all statistical business processes of the organisational units of the HCSO as well as such activities carried out on behalf of the HCSO.

3. §
Definitions

For the purpose of this Regulation, the following definitions shall apply:

1. *Data archive:* institution specialised in the acquisition, preparation and preservation of data of the society, economy and environment. The data archive serves as the main storage of historical data and carries out its activity with the purpose to make its datasets available for users.
2. *Data owner unit:* the HCSO department to which the concerned subject-matter domain belongs, according to the Operational and Organisational Rules of HCSO.

3. *Data access channel:* mode of data access, via which the users acquire data. Different conditions apply to the different data access channels.
4. *Data transfer:* ensuring access to the data for a third party. According to Act No. CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information, third party shall be any natural or legal person, or organisation without legal personality other than the data subject, the data controller or the data processor.
5. *Data protection:* legal, methodological, IT and other processes, methods and activities aimed at the protection of data from unauthorised use and misuse.
6. *Anonymised microdata:* microdata which have been modified in order to reduce to an acceptable level, in accordance with current best practices, the disclosure risk of statistical units to which they relate.
7. *Anonymised tabular data:* tabular data which have been modified in order to reduce to an acceptable level, in accordance with current best practices, the disclosure risk of statistical units to which they relate.
8. *Archiving:* safe preservation of datasets with the aim to ensure historical traceability and retrieval.
9. *Identification:* the event when the concerned statistical unit (e.g. natural person, enterprise) is clearly identified or when one or more direct identifiers of the concerned statistical unit is acquired.
10. *Safe environment:* environment, technically separated from the internal network of the data owner, the data stored in the internal network and the external network (internet), in which access to data takes place under strictly controlled conditions. In HCSO practice, safe environment covers Safe Centre access, remote access and remote execution.
11. *Individual data:* data or collection of data, describing only one statistical unit of the population, allowing direct or indirect identification of the concerned statistical unit thus providing unit-specific information.
12. *Primary cell suppression:* statistical disclosure control method applied to tabular data with the aim of not to disseminate but to replace with an agreed symbol cells marked as sensitive based on statistical disclosure control methods applied to tabular data.
13. *Disclosure:* new information on a given statistical unit (e.g. natural person, enterprise or groups of these) becoming public based on disseminated data.
14. *Disclosure risk:* joint probability of identification risk and disclosure of new information on a given statistical unit.

15. *Physical data protection:* data protection with the aim to protect data from external, physical impacts and danger, including solutions to make the access to data and devices more difficult.
16. *Data of public interest:* information or data other than personal data registered in any mode or form concerning activities undertaken and controlled by the body or individual carrying out state or local government responsibilities, as well as other public duties defined in relevant legislation, regardless of their mode of control, independent or collective nature; therefore, with special regard to data concerning the scope of authority, competence, organisational structure, professional activity and evaluation equally encompassing its effectiveness, the type of data held and legislation regulating operation, as well as data concerning financial management and concluded contracts.
17. *Direct identification:* identification of the statistical unit using direct identifiers.
18. *Direct identifier:* unique identification data or code assigned to the statistical unit (independent of the public accessibility of the code), including the denomination/name of the statistical unit, the exact address of the statistical unit (e.g. home address, site address, etc.) and the contact information of the statistical unit (e. g. e-mail address, telephone number, etc.).Technical identifiers assigned by the HCSO are not regarded as direct identifiers.
19. *Indirect identification:* identification of the statistical unit by other means than direct identification.
20. *Indirect identifier:* variable of the microdataset, which, as part of a key, might contribute to the identification of the statistical unit.
21. *Output checking:* checking of outputs produced by researchers in safe environment with the purpose to ensure that all outputs are checked by statistical disclosure control before leaving the premises of HCSO.
22. *Secondary cell suppression:* statistical disclosure control method applied to tabular data when additional cells apart from the ones treated by primary cell suppression are suppressed in order to ensure the protection of the concerned tabular data.
23. *Microdata:* record-level dataset containing information on observation units. Microdata is the main source of aggregated data.
24. *Dissemination:* making data available to any person or entity.
25. *Data request for merging/linking datasets:* data request with the purpose to merge/link dataset with other datasets. Data request for merged/linked datasets usually relate to

microdata sets where the merging/linking of datasets is performed by common key variables.

26. *Passive confidentiality:* the data of the statistical unit is protected only when the statistical unit submits a formal written request. If the data provider submits a written formal request, the data of the concerned statistical unit have to be protected by statistical disclosure control methods. In the absence of such a request, the data of the statistical unit are not to be protected. Direct identifiers of the concerned statistical units are not to be disseminated even in the absence of written request.
27. *Statistical data:* data used for the development, production and dissemination of official statistics, regardless of the source of data (statistical data collection, or data transmission and other data sources).
28. *Statistical data processing:* methods or collection of methods applied to data processed for statistical purposes, regardless of the actual methods applied; areas covered: e. g. data collection, data gathering, data capture, data systematisation, data storing, data modification, data utilisation, data transmission, data dissemination, data harmonisation, data linkage, data matching, data blocking, data deletion, data destruction and data protection.
29. *Statistical unit:* units of population with specified characteristics and attributes.
30. *Statistical disclosure control:* collection of methods used for the modification of data processed for statistical purposes in order to reduce, to the highest possible extent, the disclosure risk of statistical units to which they relate. The main purpose of statistical disclosure control is to prevent individual data to appear in the datasets.
31. *Personal data:* data related to the data subject, in particular the name and identification number of the data subject, as well as one or more factors specific to his physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data in regard to the data subject.
32. *Tabular data:* data compiled into a tabular format containing aggregated information.

4.§
The organisational setup of data protection

(1) The Data Confidentiality Board consists of legal, methodology, IT and dissemination experts, acts as a counseling and preparatory body for decision-making of the President of the HCSO and as such supervises, manages and coordinates the implementation of data protection

rules in the HCSO and also ensures the publicity of data of public interest and the protection of individual data. The members of the Board are assigned by the President of the HCSO from among the experts of the organisational units performing legal, methodological, IT and dissemination tasks. The Data Protection Commissioner of the HCSO acts as Chair of the Board. The Board:

a) Issues recommendations, opinions on methodological, legal, IT and dissemination issues related to confidentiality;
b) Participates in the preparation of internal regulations, delivers opinion on draft legislation and in justified cases initiates amendments to legislation and internal regulations of the HCSO;
c) Takes part in the management of the integrated data request management system;
d) Delivers opinion on issues related to microdata access;
e) May request information from any employee of the HCSO on issues related to confidentiality;
f) Posts its opinions, minutes of its sessions on the intranet of the HCSO.

(2) The Data Protection Commissioner of the HCSO is appointed by the President of the HCSO. The Data Protection Commissioner performs his/her tasks under the direct supervision of the President of the HCSO. The Data Protection Commissioner:

a) Prepares initiatives on the protection of individual data and the publicity of data of public interest, prepares recommendations and delivers opinion on draft legislation and internal regulations;
b) Organises training on confidentiality, assists the communication of the HCSO on confidentiality;
c) Maintains contact with employees of the HCSO performing tasks on confidentiality;
d) Prepares a yearly report for the President of the HCSO on the work of the Data Confidentiality Board and the state of the art of data protection within the HCSO;
e) Maintains contact with the Data Protection Commissioners of other institutions and organisations as well as with the National Authority for Data Protection and Freedom of Information.

(3) Each head of the organisational units appoints a confidentiality cooperative. The confidentiality cooperative:

a) Participates at the fora, trainings organised by the Data Confidentiality Board and – upon invitation form the Chair – attends the meeting of the Data Confidentiality Board;

b) Provides professional and methodological support within the organisational unit in implementing confidentiality rules and methods, and when necessary, applies statistical disclosure control methods on datasets;
c) Reviews the situation of confidentiality within the organisational unit and follows up on data access activities;
d) Acts as a contact point towards the Data Confidentiality Board regarding issues of data access of his/her organisational unit;
e) Controls and assists the proper management of the integrated data request management system at his/her organisational unit.

(4) Employees of the HCSO are responsible to follow the rules of data protection and data processing. With regard to this, they:

a) Manage and preserve the statistical data produced or learned while performing their tasks;
b) Pay attention to the security of accessed databases and registers in accordance with the internal regulations of the HCSO;
c) Adhere to the rules prescribed by legislation and internal regulations related to data processing;
d) May ask the opinion of the Data Confidentiality Board on issues related to data protection;
e) Upon start of legal relationship with the HCSO, sign a confidentiality commitment (Annex 1) on the adherence to the rules and obligations related to data protection.

(5) The heads of organisational units at the HCSO are responsible for the adherence to confidentiality rules within their unit. With regard to this, they ensure the adherence to confidentiality rules by their employees and their participation at trainings on confidentiality.

5. §

Rules related to persons in a contractual or other legal relationship with the HCSO

The heads of the organisational units ensure that all persons entering a legal relationship with the HCSO sign a confidentiality commitment. The contract concluded with the HCSO shall refer to the adherence of confidentiality rules. Annex 2 contains the form of the confidentiality commitment.

6. §

Data protection during statistical business processes

(1) Rules of data protection shall be followed during the whole statistical business process. With regard to this:

a) Physical security of data collected or taken over for statistical purposes by the HCSO has to be maintained during the whole statistical business process from the receipt of the data through any channel to the dissemination of data to users. With regard to this, data shall be protected from damage, deletion or unauthorised access. Safe storage, backup facilities and appropriate user rights management system shall also be provided.

b) During the data processing legal protection as well as application of statistical disclosure control shall be ensured besides the physical protection of the data.

c) In case of processing datasets containing personal identifiers, the direct identifiers of the statistical units used for data collection shall be stored separately from the other data. Instead of direct identifiers used for data collection, the statistical units shall be given technical identifiers, which aim at restoring the connection between the data collected and the direct identifiers used for data collection. The connection between the data and the direct identifiers used for data collection may only be restored for a given purpose, and only temporarily as long as the purpose is fulfilled. Such purpose may be the preparation and conduction of a new data collection or take over of data, further processing, validation of data, or the fulfilment of new data requests. Unless there is a valid purpose, the identifiers have to be destroyed after the data have been checked for completeness.

(2) The following data protection rules shall apply for all data collections or data transmissions of the HCSO:

a) Prior to data collection, the respondents shall be informed that the collected data will only be used for statistical purposes, during which protection of individual data is ensured.

b) The content of the completed questionnaires – apart from the respondents – shall only be made accessible to the HCSO or persons in a contractual relationship with the HCSO, performing the data collection on its behalf.

c) Technical conditions to prevent unauthorised access shall be ensured during the transportation, storage and transmission of collected questionnaires and other data carriers and data transmissions.

d) Third persons carrying out data collection on behalf of the HCSO based on legislation or an arrangement of cooperation as well as the data owner unit or the unit carrying out the data collection shall ensure the storage of the questionnaires containing individual data at a safe location and their destruction after data have been captured and checked for completeness.

e) The processing of lists of names and addresses used for data collections or transmissions shall be carried out according to the above rules.

(3) During statistical data production, the following rules shall apply:

a) Only the assigned personnel – within the scope of their respective job descriptions – or external persons, who carry out data processing on behalf of the HCSO based on a contract shall have access to final microdata and the databases which contain aggregated, raw, calculated indicators or assist data analysis and data selections or datasets which may be utilised by users. In case of external data processors, the contract shall refer to ensuring the IT and physical security of databases.

b) Access to databases containing statistical data shall be fully monitored and recorded.

c) The list of roles connected to databases as well as the list of authorised persons assigned to these roles shall be kept up-to-date in order to prevent unauthorised access.

d) The detailed rules of database access and its monitoring and documentation shall be regulated in a separate internal regulation.

(4) During the archiving of statistical data the following rules shall apply:

a) The documents (questionnaires, lists of names and addresses, direct identifiers of statistical units, etc.) used for data collection or data transmissions containing personal data shall be destroyed within one year after the target period, with the exception in 6. § (1) c).

b) The archiving of supplementary documents (metadata, questionnaires, lists of addresses, direct identifiers of statistical units used for data collection) shall be archived along with the data.

(5) The detailed rules of archiving, preservation and discard of questionnaires and other supplementary documents shall be regulated in a separate internal regulation.

7. §
Data access, dissemination

(1) Requests for statistical data may only be declined for reasons of confidentiality if the publication of data is restricted by law, therefore data access would interfere with the protection of individual data. The rules for fulfilling requests for data access of public interest as well as the detailed rules of data access channels shall be regulated in a separate internal regulation.

(2) The data of the HCSO may be accessed by users through different data access channels. The following data access channels are operated within the HCSO to provide access to data:

a) Release of tabular data: the protection of published data shall be ensured completely with statistical disclosure control, as there is no possibility of legal protection in addition to existing legislation. Relevant ways of access for published tabular data are the dissemination of data in publications, the Tables system, the Dissemination Database and the release of tabular data on individual request.

b) Release of anonymised microdata sets: In case of release of anonymised microdata sets, a microdata file is transmitted to the user. In this case it is necessary to apply legal protection measures in addition to statistical disclosure control, which together provide appropriate protection for the data. In case of release of anonymised microdata sets the rights and obligations of the user and the institution providing the anonymised microdata shall be stipulated in a contract.

c) Remote access: access in a secure environment during which access is made from designated access points via safe connection to data stored in the safe environment of the HCSO.

d) Remote execution: a data access channel through which the user transmits a syntax and/or specification to the HCSO based on which an analysis by the HCSO staff is carried out within the internal safe network of the HCSO, connected to microdata.

e) Safe Centre access: access in a safe environment, during which deidentified microdata sets are accessed on the HCSO premises.

f) Access to Public Use Files: access to microdata files with minimal risk of identification and disclosure, accessed via the internet by anyone free of charge.

(3) The individual data of HCSO is not accessible with the following exceptions.

Access to individual data may take place:

a) Based on the consent of the data provider: individual data may be transmitted if the data provider or the relevant statistical unit has given its prior informed and unambiguous written consent. The consent may only be given for a specific purpose and time period.
b) Based on the written request of the data provider concerning its own data: in case the data provider requests the transmission of its own data provided in data collection. Based on such written request, only the same data as recorded on the questionnaire may be transmitted to the data provider.
c) Based on passive confidentiality: in case European legislation establishes specific conditions on passive confidentiality, access to data processed for official statistical purposes which relates to the data provider and allows indirect identification is permitted.
d) To members of the European Statistical System or the European System of Central Banks in case the transmission of individual data is necessary for the development, production and dissemination of European statistics based on Regulation 223/2009/EC or other European legislation.
e) In case of register data defined in the Act on Official Statistics: Access to directly identifiable microdata from the registers containing data deemed public by the Act on Official Statistics may take place within the scope stipulated in the Act on Official Statistics broken down by standard categories set by the HCSO. In case the request refers to data other than the public data stipulated in the Act on Official Statistics, access may only be provided after the application of statistical disclosure control.
f) Between the organisational units of the HCSO for statistical purposes: individual data may be transmitted between the organisational units of the HCSO for statistical purposes. In this case, application of statistical disclosure control is not justified.
g) In case the data shall be considered data of public interest or data public on grounds of public interest according to the Act. No. CXII of 2011 on the right of informational self-determination and freedom of information
h) Data which is not to be considered as personal data and which may be described in natural measurement unit and may only allow indirect identification and are intended for publication within the scope of regular dissemination and that fall into the following categories:
    - railway and air transport,
    - inland waterway and overland passenger transport,
    - transport of gas and other carbon-hydrates,

- operation on airports, inland waterway and other port facilities, performance of transportation services within these facilities,
- postal services, in the framework of universal postal services, or activities replacing universal postal services, and other services performed by the universal postal service provider,
- telecommunication services,
- waste management services,
- water utility supply,
- gas, thermal energy, electricity providing services

i) Data which is not to be considered as personal data and which may be measured in value and may only allow indirect identification and are intended for publication within the scope of regular dissemination and that fall into the following categories:
   - data on the revenue from fare for rail, inland waterway and overland passenger transportation services,
   - data on the revenue from fare and freight of air transport,
   - revenue from the activity fee of telecommunication services.

(4) Access to tabular and microdata may take place:

a) For scientific purposes for Hungarian and foreign researchers under conditions set in 9. §, via any data access channel listed in 7. § (2), for any statistical data managed by the HCSO.

b) For state administration bodies, in the absence of scientific purpose, only tabular or anonymised microdata may be released with statistical disclosure control applied.

c) For data archives, tabular or anonymised microdata may only be released with statistical disclosure control applied and appropriate legal guarantees in place.

d) For international bodies outside of the European Statistical System, tabular or anonymised microdata may only be released with statistical disclosure control applied and appropriate legal guarantees in place.

e) For any other user not indicated under points a-d) – with the exception of (3) e) – may only receive tabular data with statistical disclosure control applied.

(5) In case of access in a safe environment, the data used for research shall not be transmitted to the user, who may only receive the outputs of the research. Research output must not be microdata.

(6) During the evaluation of the data request, the decision on access is made considering the available data access channels and other conditions of the request.

8. §
Management of data requests

In order to monitor the content and process of data requests, the HCSO operates an integrated data request management system. The detailed rules on the content and management of the system are stipulated in a separate internal regulation.

9. §
Statistical disclosure control of tabular data and microdata

(1) Tabular data and microdata have to be checked for confidentiality before dissemination. Regarding statistical disclosure control, the following rules apply:

a) Application of statistical disclosure control – unless an internal regulation provides otherwise – is the task and responsibility of the data owner unit.
b) Statistical disclosure control actions have to be fully documented in the integrated data request management system for the transparency and consistency of disclosure control practice.

(2) In case of release of tabular data, if primary cell suppression is applied, the necessity of secondary cell suppression shall be checked for every table and if needed, secondary cell suppression shall be applied.

(3) In case of access in secure environment, the research outputs have to be checked for confidentiality. No research outputs may be released without output checking procedure.

(4) The application of the output checking procedure, applied to research outputs produced in safe environment, – with the subject matter assistance of the data owner organisational unit – is the task and responsibility of the organisational unit performing methodological tasks.

(5) In case of data request for merged/linked datasets, only data with statistical disclosure control applied, may be released. In the absence of statistical disclosure control, the data request has to be rejected as data confidentiality is not sufficiently ensured.

(6) When applying statistical disclosure control, data to be released has to be compared to previous data releases of the same concerned statistical units in order to ensure the coherence of statistical disclosure control practice.

(7) The detailed rules of access to tabular data and microdata shall be stipulated in a separate internal regulation.

10. §

IT security and physical data protection

(1) A separate internal regulation on IT Security defines:

a) The protection methods against the dangers for the functions of the HCSO IT systems as well as the confidentiality, authenticity, intactness and continuous availability of data processed by the IT systems operated by the HCSO or in the possession of the HCSO.
b) IT actions and activities of developers, operators and users of IT systems within the HCSO.
c) Security provisions for all application levels regarding the IT systems owned or operated by the HCSO as well as the whole life cycle of their components (preparatory phase, implementation, operation, withdrawal).

(2) In order to ensure physical data protection, separate internal regulations shall apply to:

a) fire safety,
b) labour safety,
c) the secure entry of the HCSO's buildings.

11. §

Closing provisions

(1) This regulation shall enter into force on the 10th February 2017. Concurrently, the HCSO regulation 20/2015 of the President of the HCSO shall cease to have effect.

Gabriella Vukovich Dr,
President of the HCSO

Annex 1. to regulation 27/2013.

CONFIDENTIALITY COMMITMENT

I, …….. (name) (name of mother: ……, address: ……), the civil servant of the HCSO's …… Department hereby acknowledge:

I acknowledge the mandatory nature of legislation and HCSO internal regulations concerning data protection, confidentiality and IT security while performing my duties stipulated in my job description. I also acknowledge that by violating the above rules I shall have responsibility according to labour law, law on offences, civil law and penal law. I attest to having myself acquainted with Regulation 223/2009/EC of the European Parliament and the Council, the Act No. CXII of 2011. on the Right of Informational Self-Determination and on Freedom of Information, the Act No. CLV of 2016 on Official Statistics, as well as the internal regulations concerning data protection, confidentiality and IT security.

I acknowledge that it is strictly inhibited to process, disseminate or otherwise make available or use the data that has come to my knowledge while performing my professional duties.
These obligations remain in effect after the cessation of my legal relationship with the HCSO.

…….. (place), ……. (date)

……

Signature

In front of us as witnesses:

Name, signature: ……
Address: ……

Name, signature: ……
Address: ……

Annex 2. to regulation 27/2013.

CONFIDENTIALITY COMMITMENT

I, …… (name), representing ……(name of enterprise) (seat: …….., business register number: …….) Hereby acknowledge within the scope of my contract with the HCSO on …….. (objective and identification number of contract) the mandatory nature of legislation and HCSO internal regulations concerning data protection, confidentiality and IT security while performing my duties stipulated in the contract above.

I also acknowledge that by violating the above rules I shall have responsibility according to the law on offences, civil law and penal law. I attest to having myself acquainted with Regulation 223/2009/EC of the European Parliament and the Council, the Act No. CXII of 2011. on the Right of Informational Self-Determination and on Freedom of Information, the Act No. CLV of 2016 on Official Statistics, as well as the internal regulations concerning data protection, confidentiality and IT security.

I acknowledge that it is strictly inhibited to process, disseminate or otherwise make available or use the data that has come to my knowledge while performing my duties stipulated in the contract above. These obligations remain in effect after the cessation of my legal relationship with the HCSO.

…….. (place), ……. (date)

……

Signature

In front of us as witnesses:

Name, signature: ……

Address: ……

Name, signature: ……

Address: ……