**Directive No. 11/2020 of the President of the Hungarian Central Statistical Office on the Hungarian Central Statistical Office's Data Protection Regulation**

In order to ensure the protection of individual data during data processing – in accordance with Regulation 223/2009/EC on European statistics, furthermore the protection of personal data in accordance with Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter referred to as: GDPR), and the Act CLV of 2016 on Official Statistics (hereinafter referred to as: Stt.) 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**

To implement the Data Confidentiality Policy of the HCSO and to provide a common regulative framework for its data protection activities.

**2. §**

**Scope of the Regulation**

(1) The personal scope of the Regulation extends to all public service officers and employees of the HCSO (hereinafter referred to as: employees).

(2) The material scope of the Regulation extends to the all data processing of the organisational units named in (3).

(3) The explanatory provisions of these Regulation are set out in Annex 4.

**3. §**

**Data management of HCSO**

(1) In order to produce official statistics, the HCSO also manages individual data, which enables the identification of statistical units.

(2) The HCSO shall process personal data in connection with the following activities:

a) in the framework of the performance of its public task under (1), if the statistical unit is a natural person,

b) in the framework of the performance of its public task under (1), if the statistical unit is not a natural person, but the personal data of a natural person are required for contact with the statistical unit,

c) in relation to persons in government service and employment,

d) in other cases related to its organisational function in relation to its public task.

(3) Annex 3 of the Regulations (General Data Management Information) sets out the data management of the HCSO concerning personal data.

(4) In the case of data processing set out in (1) of Annex 3 to the Regulations, the rules set out in Section 6 of these Regulations shall apply.

(5) The rules of data processing concerning other personal data related to the activities of the HCSO, named in (2) of Annex 3 to the Regulations, in particular: recording, storage, access to personal data, archiving and erasure of data shall be laid down in other internal instructions governing the processes.

(6) The personal data of natural persons in government service and employment with the HCSO are processed in accordance with the HCSO's Internal Data Management Regulation.

## 4. §
## The organisational setup of data protection

**President of the HCSO**

(1) The President of the HCSO is responsible for making data protection decisions concerning the organisation.

**Data Confidentiality Board**

(2) The Data Confidentiality Board consists of legal, methodology, IT and dissemination experts, acts as a counselling 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 Officer of the HCSO acts as Chair of the Board. Its tasks are:

a) To issue recommendations, opinions on methodological, legal, IT and dissemination matters related to confidentiality;

b) To participate in the preparation of internal regulations, deliver opinions on draft legislation, and in justified cases, initiate amendments to legislation and internal regulations of the HCSO;
c) To deliver an opinion on issues related to microdata access;
d) It may request information from any employee of the HCSO on issues related to confidentiality;
e) To post its opinions and recommendations, and the minutes of its sessions on the intranet of the HCSO.

**Data Protection Officer (DPO)**

(3) The DPO of the HCSO is appointed by the President of the HCSO. The DPO performs his/her tasks under the direct supervision of the President of the HCSO. The responsibilities of the DPO are:

a) To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to GDPR and to other Union or Member State data protection provisions on the protection of individual data and the publicity of data of public interest;
b) To monitor compliance with GDPR, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data; to handle data confidentiality related breaches. To raise awareness by organising trainings on data confidentiality, by assisting the communication of the HCSO in relation to data confidentiality;
c) To maintain contact with employees of the HCSO performing tasks on data confidentiality;
d) To prepare a yearly report for the President of the HCSO on the work of the Data Confidentiality Board and the state of affairs on data protection within the HCSO;
e) To maintain contact with the DPO of other institutions and organisations as well as with the Hungarian National Authority for Data Protection and Freedom of Information with particular regard to data protection breaches.
f) To be responsible for updating these Terms.

**IT Security Officer**

(4) The IT Security Officer of the HCSO shall perform the tasks falling within its competence on the basis of legislation and the internal IT regulations of the HCSO.

**Heads of organisational units**

(5) The heads of the HCSO are responsible for the observance of data protection rules within their organisational unit. Within this framework, the head of the organisational unit ensures the observance of data protection rules and regulations, and the participation of the employees of the organisational unit in data protection training.

**Employees**

(6) All employees of the HCSO are liable for disciplinary, civil (compensation) violations and have criminal law liability for violations of data protection and data management rules. In this context, employees:

a) Manage and preserve individual and statistical data and other personal data that have become known to him or her in connection with the performance of his or her tasks;
b) In the course of her/his work, they pay attention to the security of accessed databases and register in accordance with the internal IT user regulations of the HCSO; immediately notify any data protection breach to the DPO or to any member of the Data Confidentiality Board;
c) Adhere even beyond to the above to the rules prescribed by legislation and internal regulations related to data processing;
d) May ask for the opinion of the Data Confidentiality Board on issues related to data protection in regard to data processing;
e) Upon the start of a legal relationship with the HCSO, sign a confidentiality and data protection statement (Annex 1) on the adherence to the rules and obligations related to data protection.
f) She/he must undergo the data protection training required of her/him.

**Third party**

(7) Persons (third parties) entering into a contractual or other legal relationship with the HCSO are obliged to comply with the provisions of these Regulations and the IT security rules.

(8) The heads of the organisational units shall ensure that a declaration of confidentiality and data protection is signed at the same time as the legal relationship of third parties is established. The provisions concerning the completion of the confidentiality and data protection declaration, the observance of the data protection rules, as well as the information concerning the handling of the data of the contracting party or contact persons by the HCSO must be

included in the contract with the HCSO. A model of the confidentiality and data protection statement is set out in Annex 2 of these Regulations.

**5. §**

**General rules on the protection of individual data**

(1) Statistical data protection means that individual data may only be used for statistical purposes and that individual data may not be disclosed or communicated to others unless their release is permitted by law.

(2) The physical security of data collected or received for statistical purposes by the HCSO shall be ensured during the whole Hungarian Generic Statistical Business Process Model (HGSBPM) from the receipt of the data through any channel to the dissemination of data to users. With regard to this, the data shall be protected from damage, deletion or unauthorised access. Safe storage, backup facilities and appropriate user rights management system shall also be provided.

(3) The HGSBPM consists of 8 process stages:

**Specification of needs, Design**

(4) During stages I-II of the specification of needs and design of the process model, it must be ensured that all data collection complies with the principle of proper legal authorization and purpose limitation, according to which the use of data for official statistical purposes is exclusive.

(5) Cooperation agreements recording administrative data transfers and their publicity shall be ensured.

(6) The definition of demand also refers to the definition of a specific statistical target.

(7) During the development of IT systems, the principle of built-in data protection shall be applied and the systems shall be designed in such a way as to take into account the rules and safeguards of data management.

(8) The means of protection against disclosure during the provision of information should be already designed in the specification of needs.

(9) Prior to the data collection, the respondents must be informed about data management; they should know in particular that the collected data is used only for statistical purposes, during which the HCSO ensures the protection of individual data.

**Development, Testing**

(10) During stage III of development and testing of the process model, care must be taken in the case of the acquisition and development of IT equipment to ensure that they guarantee a level of data security commensurate with the degree of security risk.

(11) A test environment should be available for IT developments and testing, and test reports should include security risk assessment and vulnerability testing.

**Data collection**

(12) During stage IV of data collection of the process model, the receipt of individual data can only take place through the IT regulation of the HCSO and a secure channel according to the relevant IT standards.

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

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

(15) Third persons carrying out data collection on behalf of the HCSO based on legislation or an agreement of cooperation as well as the data owner unit and/or the unit carrying out the data collection shall ensure the storage of the questionnaires containing individual data at a secure location and, after the data have been captured and checked for completeness – or as described in Section 5(24) –, their destruction. The organisational unit responsible for storage and destruction must be indicated in advance in the implementing instructions for data collection.

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

(17) Particular attention should be paid to the confidentiality of raw microdata files received or recorded electronically, with controlled internal access.

(18) As part of the process, data providers / data subjects should be given the opportunity to return their own data and to exercise their other rights (deletion, rectification).

(19) For the storage of all individual data, the standards ISO27001 and ISO27006 undertaken in the IT security regulations of the HCSO, as well as compliance with the IT security requirements prescribed in accordance with the provisions of the Act L of 2013.

**Data preparation, Processing**

(20) During stages V-VI of data preparation and processing of the process model, only the designated employee – within the tasks specified in his or her responsibilities – may perform the data processing for the completed micro-data and databases, collections containing aggregated, basic and calculated indicators supporting various analyses. In addition, data files that can be queried by users for the HCSO may be accessed by external persons with a contractual relationship with the HCSO. If an external data processor is used, the contract concluded with them must also cover the IT security and physical data protection of the databases that are the subject of the processing.

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

(22) The list of roles connected to databases as well as the list of authorised persons assigned to these roles shall be kept updated in order to prevent unauthorised access.

(23) Data stored in the systems may be written to an external data carrier only with the permission of the IT security officer, using the encryption procedure specified in the IT security regulations.

(24) The detailed rules of database access and its monitoring and documentation shall be defined in a separate internal regulation, the IT Service Department shall be responsible for updating the regulations.

(25) During the archiving of statistical data, the documents (questionnaires, lists of names and addresses, direct identifiers of statistical units, etc.) used for data collection or data transmissions containing personal data must be destroyed within one year after the target period, with the exception stated in Article (6) Section (15). The archiving of supplementary documents (metadata, questionnaires, lists of addresses, direct identifiers of statistical units used for data collection) should be archived along with the data. The detailed rules of archiving, preservation and discard of questionnaires and other supplementary documents are defined in a separate internal regulation.

**Preparation for dissemination, Dissemination**

(26) During stages VII-VIII of preparation for dissemination and dissemination of the process model, it should be taken into account that, for statistical purposes, the result of the data production process (statistical data) is aggregated data. Aggregated data must be examined in accordance with the HCSO's protection against disclosure before publication or data release.

(27) Analyses do not disclose the name of the data provider together with statistical data, and data that would make the data provider directly or indirectly identifiable would reveal unknown

information about them. Changes of an administrative nature in the provision of statistical data (e.g. cessation, relocation of headquarters), can be indicated in an identifiable way insofar as they have affected the development of aggregated data. The information published in the text, intertextual tables and figures of the analyses may not reveal individual data together or separately. All this must be examined in accordance with the territorial level of the analysis.

(28) During the external and internal communication of the HCSO, individual data may be transmitted only in the manner specified in the IT security regulations.

(29) The IT security officer is responsible for defining the data security rules for data storage and transmission and for recording the security requirements.

(30) Section 7 contains the external data access channels of the HCSO and their rules, as well as the legal, methodological data protection and IT security requirements of external access channels.

(31) In order to be able to trace the content and process of data releases, the HCSO keeps a unified data release register. The data content of the register and the rules of its management are determined by a separate internal legal act, and the Information Directorate is responsible for keeping it updated.

## 6. §
## Special rules on the protection of personal data

**Legal basis**

(1) The GDPR shall also apply to the processing of personal data for statistical purposes.

(2) The GDPR does not apply to the processing of data for statistical purposes if it is anonymous.

(3) The processing of personal data at the HCSO is lawful if one of the following legal basis is met:

- Consent of the data subject;
- Performance of the contract;
- Compliance with a legal obligation;
- Performance of the task carried out in the public interest;
- Legitimate interest.

(4) A mandatory provision of personal data concerning a natural person may be ordered only by law. Where a survey includes both mandatory and voluntary elements, the distinction between mandatory and voluntary responses should be clear and unambiguous.

(5) The processing of special categories of personal data for statistical purposes is permitted under Stt. taking into account Section 25 (2).

(6) The further storage of personal data may be considered lawful if it is justified and necessary for the production of statistics in order to perform a task in the public interest.

**Principles**

(7) The processing of personal data, in addition to the legal basis indicated in (3), will be lawful if it also complies with the following guarantee principles:

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality;
- Accountability;
- Data protection by design and by default;
- Security of processing.

**Rights of data subjects**

(8) The following rights of the data subjects shall be ensured for lawful data processing, subject to the provisions of (9) to (12):

- the right to information;
- right of access;
- the right to rectification;
- the right to erasure (right to be forgotten);
- the right to restrict of processing;
- the right to data portability;
- the right to object;
- the right to apply to a data protection authority;
- court redress;

(9) Under the GDPR, the right to information – with the exception of (10) – and the right of access do not apply to the processing of data for statistical purposes; moreover, the right to data portability and the right to object do not apply to the performance of a task in the public interest.

(10) The HCSO intends to exercise the right to information of data subjects by issuing the General Data Management Information. Special data management information is prepared for public data surveys.

(11) The data subject is also entitled to request information from the DPO of the HCSO.

(12) The right to restrict data processing may not be exercised by the data subject in the case of statistical data recordings if the implementation of the data collection is in accordance with the Stt.

(13) In accordance with the Stt., the data subject may exercise the right of access with respect to the data resulting from the collection of statistical data.

(14) In accordance with the Stt., the data subject may exercise his/her right to rectification in the case of statistical data collection until the start of the statistical data processing; moreover, in the case of statistical data transfer, the HCSO cannot be exercised as a recipient.

**Data security**

(15) In the case of the processing of datasets containing personal identifiers, the direct identifiers of the statistical units used for data collection shall be stored separately from the other data (pseudonymisation). Instead of direct identifiers used for data collection, the statistical units shall be given technical identifiers, which aim to restore 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 takeover of data, further processing, validation of data, or the fulfilment of new data requests. Unless there is a valid purpose, the identifiers must be destroyed after the data have been checked for completeness (anonymization).

**Personal data breach**

(16) If an employee of the HCSO detects the destruction, loss, alteration, unauthorised disclosure or unauthorised access to personal data, he or she shall immediately notify the DPO.

(17) The DPO shall ensure that the case is investigated and that the procedure prescribed by the GDPR is followed.

(18) Where the IT security incident concerns the processing of personal data, the provisions of the Security Incident Management Regulations shall apply, with the addition that the DPO shall be involved in the proceedings.

**Data protection impact assessment**

(19) A data protection impact assessment shall be carried out in advance where a processing operation, in particular using new technologies, is likely to present a high risk to the rights and freedoms of data subjects. The purpose of the data protection impact assessment is to assess the probability, sources and nature of the high risk.

(20) The head of the field or the project promoter shall ensure that the data protection impact assessment is carried out in consultation with the DPO and the head of the Statistical Coordination and Legal Department.

**Data management information**

(21) The HCSO shall issue a General Data Management Information on its permanent data management concerning personal data, the compilation, annual updating and publication of which is the responsibility of the DPO, based on the indications of the organisational units performing the data processing.

(22) The preparation, publication and updating of periodic, periodically changing data management that is not included in the General Data Management Information, especially in the case of public data surveys, is mandatory and is the task of the manager / organisational unit / project manager.

(23) In the case of joint data processing, where the HCSO and the other party are joint data controllers, the issuance of a joint data management information is justified, which clearly sets out the responsibilities.

(24) Information on the handling of personal data of natural persons in employed by the government and employed by the HCSO shall be issued by the Internal Data Management Information, and it shall be compiled, updated and published annually by the DPO on the basis of data processing organisational units.

(25) The mandatory content elements of data management information briefs are the following:

- the legal basis of data processing;
- the purpose of data processing;
- data controllers;
- data processors;
- data subject;
- the scope of the processed data;

- duration of data processing;
- data transmission;
- the rights and redress of data subjects.

**Data processors**

(26) In the course of data processing pursuant to Section 3, the HCSO may only use a data processor that certifies its data protection compliance.

(27) The processing of data pursuant to (28), its subject matter, duration, nature and purpose, the type of personal data, the categories of data subjects and the obligations and rights shall be set out in a contract (data processing agreement).

(28) For the purposes of Section 6, the terms of GDPR are applicable and used.

## 7. §
## Data access channels for users

(1) Requests for statistical data may only be declined on grounds of confidentiality if the publication of the data is restricted by law, and therefore data access would interfere with the protection of individual data.

(2) The data of the HCSO may be accessed by users through different data access channels. In order to provide the data to users, the HCSO has a general purpose in the case of points (a) to (b) below; in the case of points (c) to (f), it operates scientific data access channels

- General Purpose:

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 the existing legislation. The relevant means for everyone to access published tabular data are the dissemination of data in standard publications, the predefined tables system, the Dissemination Database and the release of tabular data on individual request.

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

- Scientific purpose (the rights and obligations of the user and the institution providing must be stipulated in a contract):

c) Release of anonymised microdata sets: during the 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 an appropriate level of data protection.

d) Remote access: access to data in a secure environment, during which data stored in the secure environment of the HCSO is accessed from designated access points via a secure connection.

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

f) Safe Centre access: access in a secure environment, during which unidentifiable microdata sets are accessed on the HCSO premises. The rules for access to the Safe Centre are laid down in a separate internal legal act, which is managed by the Information Directorate.

**Legal data protection rules for access to data**

(3) Individual data is not made public by the HCSO 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, unambiguous and deliberate 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 during data collection. Based on such written request, only the very same data content as recorded on the questionnaire may be transmitted back to the data provider.

c) Based on passive confidentiality: where European legislation establishes specific conditions and circumstances regarding passive confidentiality, access to data processed for official statistical purposes relating to the data provider and allowing indirect identification is permitted.

d) To members of the European Statistical System or the European System of Central Banks where 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 legislations.

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 reasonable.

g) In case the data is considered of public interest or public on grounds of public interest according to Act No. CXII of 2011 on the right of informational self-determination and freedom of information.

h) Data belonging to the following categories, and which are not to be considered personal data, may be described in natural measurement units, may only allow indirect identification and are intended for publication within the scope of regular dissemination:

- 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 belonging to the following categories, and which are not to be considered personal data, may be measured in value, may only allow indirect identification and are intended for publication within the scope of regular dissemination:

- 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 Section 9, via any data access channel listed in (2) Section 7, 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 with 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 with appropriate legal guarantees in place.
e) Any other user not indicated under points a-d) – with the exception of (3) e) – may only receive tabular data with full statistical disclosure control applied.

(5) In case of access to data in a secure environment, the microdata used for research shall not be transmitted to the user, only the research outputs should be made available for the data requestor. Research output must not be microdata.

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

(7) The order of the above data access and the detailed rules of the data access channels are determined by the data access regulations, the Information Directorate is responsible for updating the regulations.

**Methodological data protection rules for access to data**

(8) Tabular data and microdata have to be fully checked for protection of confidentiality prior to 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 transparency and consistency with disclosure control practices.

(9) 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.

(10) 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.

(11) The execution of the output checking procedure, applied to research outputs produced in a secure environment, – with professional assistance of the data owner organisational unit – is the task and responsibility of the organisational unit performing methodological tasks.

(12) 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 on the grounds of data confidentiality not being sufficiently ensured.

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

(14) The detailed rules of access to tabular data and microdata are stipulated in the data access regulation, for which the Information Directorate is responsible.

**IT data protection rules for data access**

(15) The IT security rules for external data access are defined in the data access policy, which is managed by the Information Directorate.

## 8. §
## Rules on data of public interest

(1) The Stt. provides that data produced for official statistics are public, but individual data may not be disclosed. However, individual data may be exceptionally released if it is in the public interest.

(2) Act CXII of 2011 (Section 5-6, points 5-6 of the Information Act) contains the concepts of public data and public data in the public interest.

(3) The determination of the public interest of the data is the task of the organisational unit of the data owner, it must be considered and interpreted on the basis of the definition of the concept whether it is included or not.

(4) In the case of public data in the public interest, it can be found exactly in the text of an act, with the expression that the data or register is public.

(5) If it cannot be established beyond reasonable doubt that a data is in the public interest, in particular because it cannot be separated from other non-public data during the statistical data production process, the data request may be rejected.

## 9. §
## Contact rules

**Enforcement of the rights of the data subject**

(1) In the event of a violation of the data subject's right to the protection of personal data, he or she is entitled to refer to the DPO of the HCSO, who is obliged to investigate and inform the data subject.

(2) The data subject has the right to refer to the DPO in connection with the data processing named in the General Data Management Information of the HCSO, or primarily, but not exclusively to the contact person indicated therein.

(3) In the case of (2), the data subject shall be informed by the head of the organisational unit / project concerned by the data processing, taking into account the professional opinion of the DPO and, if necessary, the Data Confidentiality Board.

**Request for data of public interest**

(4) Anyone may submit a request for data of public interest to our Office in person at the reception time, by telephone or e-mail at the official contact details, or electronically via the Contact Us interface on the website.

(5) The Information Act shall govern the fulfilment of requests for access to data of public interest.

**Statistical data requests**

(6) Anyone can request statistical data managed by the HCSO in person during reception time, by phone or e-mail at the official contact details, or electronically via the Contact us interface on the website.

## 10. §
## IT security and physical data protection

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

a) The protection methods against the dangers threatening the functions of the HCSO IT systems as well as the confidentiality, authenticity, integrity 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 from the system).

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

a) fire safety,

b) occupational safety,

c) secure entry into and exit from the HCSO's buildings.

**11. §**

**Closing provisions**

(1) This regulation shall enter into force on 9 June 2020.

(2) Concurrently, the HCSO regulation 27/2013 on data protection regulations of the HCSO and its amending regulations 10/2018 and 23/2019 shall be revoked.

*Gabriella Vukovich Dr*,
President of the HCSO