BÉKÉSCSABA, CITY OF COUNTY RANK

AND

THE MAYOR'S OFFICE OF BÉKÉSCSABA

DATA PROTECTION POLICY

AND

DATA PROTECTION REGULATIONS

DATA PROTECTION POLICY AND DATA PROTECTION REGULATIONS OF BÉKÉSCSABA, CITY OF COUNTY RANK AND THE MAYOR'S OFFICE OF BÉKÉSCSABA

The Local Government of Békéscsaba and the Mayor's Office of Békéscsaba, which performs the administrative tasks of the Local Government - in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: GDPR) - considering that the Office processes a significant amount of personal data, considers the protection of personal data to be of paramount importance.

The Office strives to ensure that - in order to fully implement the principle of purpose limitation and data minimization formulated in the GDPR - only those persons who need to access personal data and **only to the extent absolutely necessary for the performance of the given task can access them**.

The Office is committed to establishing and **operating solutions and procedures** that ensure compliance with the requirements of the GDPR and domestic data protection standards, and makes every effort to protect the personal data it processes from unauthorized access using **appropriate security technologies and procedures**.

The Office pays special attention to **cooperating with partners** who ensure compliance with the applicable data protection rules at all times, as well as the protection of the rights of data subjects.

The Office makes every effort to ensure that its customers, employees, partners and all other data subjects **have adequate knowledge** of the processing of their personal data by the Office and the rules governing data processing, and that all data subjects **can properly exercise their rights related to their personal data**.

In order to ensure continuous compliance with the regulations, the Office strives to apply methods that reassuringly ensure the **regular review and development** of solutions, procedures and technical background related to data processing.

We trust that the processing of personal data according to the above aspects will also contribute to the Office performing its tasks in accordance with the law, to the satisfaction of the population of Békéscsaba.

The most important information, applicable laws and regulations, as well as the contact details of the data protection officer regarding the Office's data processing activities are available on the Office's website (www.bekescsaba.hu) under the Data Protection menu item.

Békéscsaba, 2020. július 27.

Szarvas Péter
polgármester

Dr. Bacsa Vendel
jegyző

DATA PROTECTION POLICY AND DATA PROTECTION REGULATIONS OF BÉKÉSCSABA, CITY OF COUNTY RANK AND THE MAYOR'S OFFICE OF BÉKÉSCSABA

The Local Government of Békéscsaba (hereinafter referred to as the Local Government) and the Mayor's Office of Békéscsaba (hereinafter referred to as the Office), in order to regulate the processing of personal data during their operation - in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46 (hereinafter: GDPR), and Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter: Info Act) - we issue this Regulation in the interest of protecting the data of natural persons:

Part I

INTRODUCTORY PROVISIONS

I/1. Purpose of the Regulation

The purpose of this Regulation is to establish internal rules and procedures and to provide a basis for individual measures that ensure that the activities of the Local Government and the Office - which performs the administrative tasks of the Local Government - comply with the applicable provisions of the GDPR and the Info Act, and facilitate the exercise of the rights of data subjects, thereby implementing a comprehensive data protection mechanism covering the entire activity of the Local Government and the Office.

I/2. Data Controller

Pursuant to Section 84 of Act CLXXXIX of 2011 on Local Governments of Hungary (hereinafter: Mötv.), the Local Government, pursuant to Section 80 of Act CLXXIX of 2011 on the Rights of Nationalities, the local minority self-governments of Békéscsaba, pursuant to Section 95(4) of the Mötv., the Békéscsaba and Region Multi-Purpose Local Government Association for administrative purposes, and pursuant to Resolution 325/2012 (XI. 23.) of the General Assembly of the Local Government of Békéscsaba, the Munkácsy Mihály Museum, certain administrative tasks are performed by the Office, and therefore the Office is considered the data controller.

The official name of the data controller is: Mayor's Office of Békéscsaba;

registered office: 5600 Békéscsaba, Szent István tér 7.;

legal status: budgetary body of the local government (municipal office);

telephone number: 66/523-800;

e-mail address: varoshaza@bekescsaba.hu.

I/3. Scope of the Regulation

This Regulation applies to the processing [GDPR Article 4(2)] of personal data [GDPR Article 4(1)] processed or recorded by the Office in the course of its competence and performance of duties.

Accordingly, this Regulation applies to all administrative and case management procedures involving personal data in the Office, and to all physical and IT equipment used in the course of data processing, regardless of their location and ownership status.

The provisions of this Regulation shall be applied by all persons who are in an employment relationship with the Local Government and the Office for the purpose of performing work, and who process personal data in the course of performing their duties or the contract governing their employment relationship, regardless of whether they perform their work within the framework of a public service relationship, employment relationship or other employment relationship (hereinafter: employees).

With reference to point I/2 of this Regulation, employees of the following organizations must also apply the provisions of this Regulation in the course of performing their duties:

a) Polish Minority Self-Government of Békéscsaba; b) German Minority Self-Government of Békéscsaba; c) Roma Minority Self-Government of Békéscsaba; d) Romanian Self-Government of Békéscsaba; e) Slovak Self-Government of Békéscsaba; f) Ukrainian Self-Government of Békéscsaba; g) Munkácsy Mihály Museum and h) Békéscsaba and Region Multi-Purpose Micro-Regional Local Government Association.

1/4. Definitions

For the purposes of this policy:

a) **Personal Data:** Any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person [GDPR Article 4(1)].

b) **Data Processing:** Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction [GDPR Article 4(2)].

c) **Restriction of Data Processing:** The marking of stored personal data with the aim of limiting their processing in the future [GDPR Article 4(3)].

d) **Profiling:** Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements [GDPR Article 4(4)].

e) **Pseudonymization:** The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person [GDPR Article 4(5)].

f) **Filing System:** Any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized, or dispersed on a functional or geographical basis [GDPR Article 4(6)].

g) **Data Controller:** The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law [GDPR Article 4(7)].

h) **Data Processor:** A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller [GDPR Article 4(8)].

i) **Recipient:** A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal

data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing [GDPR Article 4(9)].

j) **Third Party:** A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data [GDPR Article 4(10)].

k) **Consent of the Data Subject:** Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her [GDPR Article 4(11)].

l) **Data Breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed [GDPR Article 4(12)].

1/5.Principles

1. Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject (principle of fair and lawful processing) [GDPR Article 5(1)(a)].
2. Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle) [GDPR Article 5(1)(b)].
3. Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (data minimization principle) [GDPR Article 5(1)(c)].
4. Personal data must be accurate and, where necessary, kept up to date (accuracy principle) [GDPR Article 5(1)(d)].
5. Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation principle) [GDPR Article 5(1)(e)].
6. Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures (integrity and confidentiality principle) [GDPR Article 5(1)(f)].
7. The controller shall be responsible for, and be able to demonstrate compliance with, the principles laid down in this policy. Accordingly, employees shall also be obliged to act in such a way that, if necessary, they are able to demonstrate compliance with the principles at the request of their superior (accountability principle) [GDPR Article 5(2)].

1/6. Tasks related to data processing

1. The Mayor

   a) Based on the proposal of the notary public, submits to the General Assembly of the Municipality of Békéscsaba proposals for resolutions or draft decrees to ensure the personal and material conditions necessary for the operation of the data protection mechanism of the Office or the Municipality established by these rules.

b) When preparing the draft budget decree, keeps in mind the need to ensure the conditions necessary for compliance with national and European data protection legislation.

2. The notary public

a) Develops the appropriate organizational structure of the Office, also taking into account the enforcement of national and European data protection laws.

b) Ensures that the positions specified in the Office's basic documents are filled.

c) Ensures the issuance of the necessary internal regulations and instructions, also taking into account the enforcement of national and European data protection laws.

d) Appoints the data protection officer.

3. Heads of organizational units of the Office

a) Continuously inform employees about the applicable national and European data protection laws.

b) Give instructions addressed to employees in light of the applicable national and European data protection laws.

4. Head of Human Resources Group

a) Ensures that when a new employee is hired, the employee is made aware of the provisions of these rules, and that this is properly documented.

b) Cooperates with the data protection officer.

5. Head of IT Group

a) Ensures the operation of the IT system based on these rules and the laws and internal regulations on IT security.

b) Ensures that the data stored on the servers are protected against unauthorized access, modification, or destruction.

c) Together with his/her direct colleagues, provides assistance to the Office staff in solving technical problems related to the fulfillment of the requirements of these rules.

6. Employees

a) In the course of their official duties, they are obliged to fully comply with the applicable national and EU data protection laws, in particular the provisions of the GDPR and the Info Act.

b) They are obliged to keep confidential the personal data they become aware of in connection with their work.

c) In the event of legal interpretation questions arising in connection with data processing, they are obliged to initiate consultation with the data protection officer without delay.

d) In the event of a data protection incident occurring, expected to occur, or suspected to have occurred, they are obliged to notify the data protection officer and the notary public in accordance with the procedure set out in these Rules.

e) They are obliged to remedy any irregularities discovered in connection with data processing without delay.

f) They are obliged to immediately report any malfunction of computer equipment or any problem in the manageability of the processed data to the head of the IT Group.

g) They are obliged to attend the data protection training organized in the Office.

PART II: LEGAL BASIS FOR DATA PROCESSING

Personal data may only be processed if any of the legal bases defined in the GDPR and below are demonstrably in place.

II/1. Consent of the data subject

Consent is any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Consent must be obtained before the processing begins.

Accordingly:

a) Employees must provide the data subject with adequate information about the processing;

b) Consent must always be given by an active act or statement in writing, orally or electronically;

c) Employees must be able to demonstrate at any time during the processing that the data subject has consented to the processing;

d) It must be ensured that the data subject can withdraw his/her consent at any time, and withdrawal of consent must be made as easy as giving it.

II/2. Data processing based on a contractual relationship

In the case of data processing based on a contract, the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into the contract.

In the case of data processing based on a contract, special attention must also be paid to the principle of data minimization. Accordingly, personal data may only be included in a contract and processed in connection with a contract to the extent necessary for the performance of the contract.

II/3. Data processing in connection with the fulfillment of a legal obligation

Personal data may be processed if the processing is necessary for compliance with a legal obligation to which the controller is subject.

In the case of data processing based on a legal obligation, the scope of the data to be processed, the purpose of the processing, the duration of the storage of the data, and the recipients are governed by the provisions of the underlying legislation.

In the case of data processing carried out on this legal basis, employees must always be able to demonstrate that the legal obligation is prescribed by a valid law. If the relevant legislation changes, it must be examined whether the legal basis for the processing of personal data still exists.

II/4. Data processing based on vital interest ("vis maior")

Personal data may be processed if it is necessary to protect the vital interests of the data subject or of another natural person. Data processing on this legal basis may only be carried out if and for as long as it is not possible on any other legal basis and it is shown to be necessary and proportionate [GDPR Recital 46].

II/5. Performance of a task carried out in the public interest and exercise of official authority

Personal data may be processed if the processing is necessary for the performance ofa task carried out in the public interest or in the exercise of official authority vested in the controller.

In the case of data processing carried out on this legal basis, employees must always be able to demonstrate that the public interest or official authority is prescribed by a valid law. If the relevant legislation changes, it must be examined whether the legal basis for the processing of personal data still exists.

II/6. Data processing based on legitimate interest

Personal data may be processed if it is necessary for the purposes of the legitimate interests pursued by the controlleror by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child [GDPR Article 6(1)(f)].

PART III: GENERAL RULES ON DATA PROCESSING

The Office clerks may only process personal data in the course of their duties in compliance with the applicable national and EU legislation and the provisions of these rules. Special care must be taken to comply with data protection rules when processing the personal data of persons under the age of 16.

The staff of the Office shall be subject to disciplinary, liability, regulatory and criminal liability for the lawful processing of personal data of which they become aware in the course of their work.

The Office shall store the personal data processed in the course of its duties for the period specified in the sectoral legislation applicable to the given type of case or in accordance with the current rules on records management.

Paper or digital copies of documents containing personal data may only be made for justifiable purposes. Copies may be kept until the purpose of the copying is achieved, but no longer than the destruction of the original document as specified in the file plan.

Separate regulations shall be in place on the IT security and data protection rules applicable to the Office, on the data protection rules relating to files, and on the data protection and IT security rules relating to the public service register containing the personal data of persons employed by the Office.

The Office shall inform data subjects of the most basic data protection rules, the contents of these rules and the remedies available to them

a) on the city's website;

b) on the Office's notice board and

c) through its staff.

The Office does not process biometric data.

The Office does not transfer data to third countries.

The Office does not engage in automated decision-making.

PART IV:

RIGHTS OF DATA SUBJECTS

IV/1. Right to information

Data subjects must be provided with adequate information - in a so-called proactive manner (in advance) - about the fact of the data processing and other information relating to the data processing, including in particular:

- the identity and contact details of the controller and its representative;
- the purposes and legal basis of the processing;
- the categories of personal data concerned;
- the fact and circumstances of any transfer of data abroad;
- the data retention period;
- the duration of the processing;
- the rights of the data subject;
- where the processing is based on consent, the possibility and means of withdrawing consent;
- where the data have not been obtained from the data subject, the source of the data;
- the technical and organisational measures taken to protect the data;
- the remedies available to the data subject;
- the identity and contact details of the data protection officer.

The information shall be provided in an intelligible form. If necessary, the data subject shall be provided with the applicable national and European data protection legislation and the Office's data protection regulations.

IV/2. Right of access

The data subject must be provided with feedback - upon request - during the processing of the data on:

- the scope of the personal data processed;
- the purpose of the data processing;
- the categories of personal data processed;
- the recipients or categories of recipients of the personal data;
- the fact and circumstances of any transfer of data abroad;
- the data retention period;

- the rights of the data subject;
- the source of the data;
- the remedies available to the data subject.

The feedback shall be provided in an intelligible form. If necessary, the data subject shall be provided with the applicable national and European data protection legislation and the Office's data protection regulations.

IV/3. Right to rectification

In order to enforce the principle of accurate and up-to-date data processing, the Office is obliged to rectify inaccurate personal data concerning him or her without undue delay at the request of the data subject.

At the request of the data subject, the Office is obliged to complete incomplete personal data without undue delay, but in doing so, the principle of purpose limitation and data minimization must be taken into account.

If the rectification was requested by the data subject, he/she must be informed of the rectification or, if applicable, of the refusal - together with the reasons for the refusal - without delay, but no later than 30 days after receipt of the request, in a documented form.

If the Office has transferred the personal data requested to be rectified or completed to a processor or, in the case of joint controllership, to another controller, the processor or the other controller must be informed without delay of the rectification or completion of the data, unless this proves impossible or involves disproportionate effort. The data subject shall be informed of such recipients upon request.

IV/4. Right to erasure ('right to be forgotten')

At the request of the data subject, the Office is obliged to erase personal data concerning him or her without undue delay (right to erasure) if any of the following reasons apply:

a) the personal data are no longer necessary in relation to the purposes for which they were processed;

b) in the case of processing based on consent, the data subject withdraws consent, provided that there is no other legal basis for the processing;

c) the data subject objects to the automated processing, provided that there is no overriding legitimate reason for the processing;

d) the Office has processed the personal data unlawfully;

e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the Office is subject.

In the event of erasure, it must be ensured that the erased data cannot be recovered in electronic systems.

The erasure must be recorded in minutes. The minutes must be completed in such a way that the deleted personal data are not included (the minutes should only refer to the scope of the data). The minutes must be sent to the data protection officer without delay, who shall keep a record of the erasure minutes in a registered file.

If the erasure was requested by the data subject, he/she must be informed of the erasure or, if applicable, of the refusal - together with the reasons for the refusal - without delay, but no later than 30 days after receipt of the request, in a documented form.

If the Office has transferred the personal data requested to be erased to a processor or, in the case of joint controllership, to another controller, the processor or the other controller must be informed without delay of the erasure of the data, unless this proves impossible or involves disproportionate effort. The data subject shall be informed of such recipients upon request.

Where the Office has made personal data public and is obliged to erase it pursuant to the GDPR and these rules, it shall take reasonable steps, including technical measures, taking into account available technology and the cost of implementation, to inform controllers processing the data that the data subject has requested the erasure of any links to, or copy or replication of, those personal data ('right to be forgotten').

IV/5. Right to restriction of processing (blocking)

At the request of the data subject, the Office shall without undue delay restrict the processing if

- the accuracy of the personal data is contested by the data subject (the restriction shall apply for the shortest possible period which allows the Office to verify the accuracy of the personal data);
- the processing is unlawful and the data subject opposes erasure of the personal data and requests the restriction of their use instead;
- the Office no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the purposes of the establishment, exercise or defence of legal claims;
- the data subject has objected to processing (the restriction shall apply for the shortest possible period which allows the Office to verify whether the legitimate grounds of the Office override those of the data subject).

In the case of restriction, the head of the organisational unit actually carrying out the processing shall, after consultation with the data protection officer and, if necessary, the head of the IT Group, designate the persons responsible and give instructions for the implementation of the restriction.

In the case of restriction, it must be ensured that the deleted data are restricted in electronic systems. The restriction must be recorded in minutes. The minutes must be completed in such a way that the restricted personal data are not included (the minutes should only refer to the scope of the data). The minutes must be sent to the data protection officer without delay, who shall keep a record of the restriction minutes in a registered file.

If the restriction was requested by the data subject, he/she must be informed of the restriction or, if applicable, of the refusal - together with the reasons for the refusal - without delay, but no later than 30 days after receipt of the request, in a documented form.

If the Office has transferred the personal data requested to be restricted to a processor or, in the case of joint controllership, to another controller, the processor or the other controller must be informed without delay of the restriction of the data, unless this proves impossible or involves disproportionate effort. The data subject shall be informed of such recipients upon request.

IV/6. Right to data portability

At the request of the data subject, the Office shall provide the personal data concerning him or her in a structured, commonly used and machine-readable format, provided that

- the processing is based on consent or on a contract and
- the processing is carried out by automated means.

IV/7. Right to object

The data subject shall have the right to object, on grounds relating to his or her particular situation, to processing of personal data concerning him or her which is based on a task carried out in the public interest or in the exercise of official authority or on the legitimate interests of the controller or a third party.

If the Office finds the objection to be well founded, it shall terminate the processing.

In the event of an objection, the data may only be processed further if the Office can demonstrate that the processing is justified by compelling legitimate grounds which override the interests, rights and freedoms of the data subject or which relate to the establishment, exercise or defence of legal claims.

In the event of an objection by the data subject, the data subject shall be informed without delay, but no later than 30 days after receipt of the objection, in a documented form, together with the reasons for any refusal.

IV/8. Right to lodge a complaint with a supervisory authority

Any person may lodge a complaint with a supervisory authority on the grounds that a breach of the law relating to the processing of personal data has occurred or is likely to occur.

The name of the supervisory authority is:

National Authority for Data Protection and Freedom of Information;

its registered office is at 1125 Budapest, Szilágyi Erzsébet fasor 22/C;

its telephone number is 1/391-1400;

its fax number is 1/391-1410;

its e-mail address is ugyfelszolgalat@naih.hu

IV/9. Judicial remedy

The data subject may bring an action before the court against the Office if he/she considers that his/her personal data are being processed by the Office or by a data processor mandated or acting on its behalf in breach of the provisions of the law or of a binding legal act of the European Union on the processing of personal data.

The Gyula District Court has jurisdiction in the case, but the action may also be brought before the district court of the data subject's place of residence or stay.

The registered office of the Gyula District Court is: 5700 Gyula, Béke sgt. 38;

telephone number: 66/562-200.

PART V

RULES ON SPECIFIC DATA PROCESSING OPERATIONS

V/1. Provisions on personal identification and identity documents

The identification of data subjects may only be carried out by presenting one of the official identity cards suitable for proving identity (hereinafter referred to as "identity document") as defined in Act LXVI of 1992 on the registration of personal data and addresses of citizens or by applying one of the identification methods specified in Act XX of 1996 on the identification methods replacing the personal identification mark and the use of identification codes.

The eleven-digit personal identification number may not be processed without legal authorization, even with the express consent of the data subject.

In accordance with the principles of necessity and data minimization, photographs or copies of identity documents may only be made if this is mandatory by law. The data subject must be informed of the fact of copying before copying.

V/2. Use of image and sound recording devices

In view of the fact that the applicable national and European data protection legislation must also be applied to images and sound recordings; recording of images and sound recordings in the course of official work is only possible if it is necessary and proportionate and the controller has an appropriate legal basis for doing so.

When using image and sound recording devices, data subjects must be informed of the fact of the image or sound recording, or - in the case of consent as a legal basis - the consent of the data subject to the making of the image or sound recording must be obtained in a verifiable manner.

Image and sound recordings should primarily be made in the course of work using technical equipment owned by the Municipality or the Office (camera, video camera, dictaphone, computer, tablet, mobile phone, etc.). If the image or sound recording is not made with technical equipment owned by the Municipality or the Office (privately owned technical equipment), the image or sound recording must be copied to an official storage medium or technical device as soon as possible, and at the same time the image or sound recording must be deleted from the privately owned technical device in such a way that it can no longer be recovered.

Images and sound recordings containing personal data may only be made public if this is expressly permitted by law or if the data subject has given his or her prior consent in a verifiable manner.

Image or sound recording equipment owned by the Municipality or the Office may only be handed over to another person by the official using it if there are no images or sound recordings containing personal data on the device or on the storage medium placed in it.

Images and sound recordings containing personal data may only be retained for as long as all of the following conditions are met:

a) the legal basis for the processing exists;

b) the retention of the image and sound recording is necessary and proportionate;

c) the retention period of the file for the case has not expired.

Sound recordings are made of the proceedings of the meetings of the General Assembly of Békéscsaba County Municipality, the committees of the General Assembly, the local governments of the settlements, the council of the association of the micro-regional association and its committee(s) (hereinafter together: the meetings of the general assembly and its bodies), and sound recordings may be made of the proceedings of the meetings of other bodies, working groups and consultations. The legal basis for the processing is: processing necessary for compliance with a legal obligation, performance of a public task or legitimate interest.

Sound recordings made at the meetings of the general assembly and its bodies shall be considered minutes, to which the rules on the preservation of paper minutes shall apply mutatis mutandis.

The person presiding over the meeting or the official making the sound recording is obliged to draw the attention of those present to the fact that the sound recording is being made. The fact that the sound recording is being made should also be included in the invitation to the meeting, if possible.

The Office has a security camera system in operation, the use of which is governed by the provisions of these rules and the provisions of a separate regulation on the use of the system.

V/3. Recording of telephone conversations

Telephone conversations may only be recorded in the course of official work in justified cases and after prior notification of all parties to the telephone conversation.

V/4. Image and sound recordings of the Office staff made by third parties

In the course of performing their duties as set out in their job descriptions, the staff of the Office are obliged to attend a number of events at which they are considered public figures. These include, in particular:

- staff members participating as performers in the meetings of the general assembly and its bodies and in the meetings of the local minority self-governments;
- staff members of the Office participating as press officers, protocol officers, or experts in press conferences organized by the Office, the Municipality, or the minority self-governments;
- registrars and family event organizers participating in family events organized by the Office;
- staff members participating as part of their official duties in youth, educational, cultural, sports, minority and community events, celebrations and commemorations organized or co-organized by the Office, the Municipality or the local minority self-governments;
- electoral office staff participating in the work of the electoral bodies that can be recorded by the press during the electoral process;
- staff members of the Office involved in the implementation of investments or tenders, participating in public and press-open events (project opening and closing events, foundation stone laying ceremonies, site visits, technical handover inspections, building inaugurations, handover ceremonies, etc.);
- staff members of the Office participating as speakers or organizers in press-open conferences, professional lectures and presentations organized or co-organized by the Office, the Municipality or the local minority self-governments;

- staff members participating in the organization or running of professional exhibitions and fairs organized or co-organized by the Office, the Municipality or the local minority self-governments;
- staff members of the Office present on behalf of the Office, the Municipality or the local minority self-governments as invitees to public or press-open domestic or foreign programmes (conferences, exhibitions, twin-town events, etc.) organized by other organizations or persons.

At the events listed above, press officers and other third parties may take photographs and/or make sound recordings without special permission, and may make these recordings public. The staff of the Office are obliged to tolerate the making of such recordings. The legal basis for the processing is: performance of a contractual obligation or legitimate interest.

At the events listed above, the employer (Office) or the employer's representative is also entitled to take photographs and/or make sound recordings. The recordings will be used, if necessary, for

a) preservation;

b) publication in the press, on websites, on social networking sites, in city marketing and city information publications;

c) sending to third parties (e.g. the issuer, manager, contributor, etc. of the tender) [hereinafter: a)-c) together: use]. The staff of the Office are obliged to tolerate the making and use of photographs and/or sound recordings. The legal basis for the processing is: performance of a contractual obligation, legitimate interest, or performance of a public task.

V/5. Data processing in connection with the meetings of the general assembly and its bodies

The submissions and their annexes prepared for the meetings of the general assembly and its bodies may only contain personal data to the extent absolutely necessary for decision-making.

If the data subject has not consented to the disclosure of his/her personal data, the personal data may not be included in the submission prepared for the public meeting. When requesting consent, special attention must be drawn to the fact that the submissions for public meetings are published on the city's website and thus become available to anyone without restriction.

If the data subject has not consented to the disclosure of his/her personal data, the decision must be anonymised before it is published on the website.

Submissions prepared for closed meetings must be clearly marked as closed. If necessary, in particular in the case of processing of special categories of data, special attention must be drawn to the rules on the processing of personal data.

V/6. Provisions on electronic mail (e-mail)

In view of the fact that electronic mail sent and received in the course of official work may contain personal data, and that the e-mail addresses of the senders of incoming electronic mail or the recipients of outgoing electronic mail may also be personal data, the sending and receiving of electronic mail must also be carried out in full compliance with the applicable national and EU data protection legislation.

Only official (....@bekescsaba.hu) e-mail addresses may be used for official work.

Incoming messages to official e-mail addresses may only be forwarded to non-official e-mail addresses in justified cases and with the permission of the notary public. The forwarding must be initiated through

the head of the IT Group. The head of the IT Group shall keep a record of the permissions granted. The head of the IT Group is obliged to review the necessity of the authorized forwarding at least once a year and, if the forwarding is found to be unnecessary, to make a proposal to the notary public to withdraw the authorization for the forwarding.

Official e-mail boxes may only be made accessible on mobile devices with the permission of the notary public. The access must be initiated through the head of the IT Group. The head of the IT Group shall keep a record of the permissions granted. The head of the IT Group is obliged to review the necessity of the authorized access at least once a year and, if the access is found to be unnecessary, to make a proposal to the notary public to withdraw the authorization for the access.

Mobile devices from which official e-mail boxes have been made accessible must be protected from unauthorized access by a password (PIN code) or biometric identifier (fingerprint) at all times.

Office staff are obliged to review the folders of their official e-mail addresses at least once a year and to delete any messages containing personal data or sent to or received from e-mail addresses that are considered personal data and which relate to files that have already been destroyed under the applicable records management legislation.

If office staff send an e-mail to several data subjects, they are obliged to do so in such a way that the data subjects do not know each other's e-mail addresses, which are considered personal data (by sending the e-mail as separate messages or by using the "blind carbon copy" function).

A communication containing personal data may only be sent by e-mail if the employee has ascertained that the user of the e-mail address indicated as the recipient is entitled to know the personal data contained in the communication.

V/7. Handling of office waste paper

Paper waste containing personal data generated during office work may only be placed in the "normal" (municipal) office waste bins if all personal data on it has been made unrecognizable - by using a paper shredder or by other means. If the personal data cannot be made unrecognizable due to its quantity or any other reason, the paper waste must be handled separately (in a paper bag) and the packaging (paper bag) must indicate the confidential nature of the documents. The paper bag must be handed over sealed to the office worker or contractor who is carrying out the destruction.

Contracts for the destruction of office waste paper may only be concluded with contractors who are able to comply with the requirements of the applicable national and EU data protection legislation for data processors.

V/8. Handling of computer data carriers

Computer data storage devices (CDs, DVDs, pen drives, external hard drives, SD cards, etc.) cannot be placed in "normal" (municipal) waste bins in accordance with the requirements of the IT security policy and environmental considerations.

Devices that are no longer used, damaged or intended for destruction must be handed over to the IT Group. The IT Group and the Municipal Services Department shall ensure the destruction of the equipment and/or the rendering of the data stored on it unreadable, with the involvement of an external contractor if necessary.

Contracts for the destruction of computer data carriers may only be concluded with contractors who are able to comply with the requirements of the applicable national and EU data protection legislation for data processors.

PART VI

RECORDS OF PROCESSING

ACTIVITIES VI/1. General rules for the record of processing activities

The data protection officer shall maintain an up-to-date record of the Office's processing activities. The heads of the Office's organisational units and the Office's staff shall be obliged to provide the information necessary for the data protection register without delay at the request of the data protection officer.

VI/2. Content of the record of processing activities

The record of processing activities shall contain the following information in a transparent (tabular) form:

1. the name and contact details of the controller; in the case of joint controllership, the name and contact details of the joint controller;
2. the name and contact details of the controller's (and joint controller's) representative and data protection officer;
3. the organisational unit of the Office involved in the processing;
4. the purpose of each processing operation;
5. the scope of the personal data processed;
6. the legal basis for the processing;
7. the categories of recipients to whom the personal data are or will be disclosed;
8. where possible, the envisaged time limits for erasure of the data;
9. where applicable, a general description of the technical and organisational measures to ensure appropriate data security;
10. other comments.

PART VII

DATA BREACH

In the event of a data breach, the employee actually carrying out the processing or the employee who detects the data breach shall immediately report the occurrence of the data breach to the notary public through his/her supervisor and directly to the data protection officer.

At the request of the data protection officer, the employee shall, without delay, provide information on the circumstances of the data breach (in particular, the identity of the data subject, the scope of the personal data processed, the act or omission constituting the data breach, and how the data breach became known), including, where necessary, by providing a copy of the document.

The data protection officer shall, without undue delay and at the latest within 72 hours of the controller becoming aware of it, notify the personal data breach to the supervisory authority (National Authority for Data Protection and Freedom of Information) using the online interface provided for this purpose, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The data protection officer shall, without undue delay, but at the latest after notification of the personal data breach to the supervisory authority, propose to the notary public and to the employee actually carrying out the processing and his/her immediate superior the necessary data protection measures to be taken. If necessary, the data protection officer shall make a proposal for action after consultation with the head of the IT Group and/or the head of the Human Resources Group.

If necessary, the data protection officer shall, after an appropriate period of time, check the implementation of the measures ordered on the basis of his/her proposal, the compliance with the rules on the processing of the personal data of the persons concerned by the data breach, and shall inform the notary public of the findings of the check.

The data protection officer shall keep a register of personal data breaches, which shall contain:

a) the scope of the personal data concerned;

b) the number of persons affected by the personal data breach;

c) the date of the personal data breach;

d) the circumstances and effects of the personal data breach;

e) the time of notification to the supervisory authority or the justification for not notifying;

f) the measures taken to remedy the personal data breach;

g) other comments.

PART VIII

DATA PROTECTION OFFICER

VIII/1. Appointment and status of the data protection officer

The notary public shall designate a data protection officer from among the staff. The data protection officer may be a public official who has sufficient knowledge of the functioning of the Office and a sufficient level of knowledge of national and European data protection legislation and practices.

The name, telephone number and e-mail address of the data protection officer shall be made available at least once after his or her appointment - in the Csabai Mérleg, the city's newspaper, and continuously after his or her appointment on the www.bekescsaba.hu website (hereinafter: the city's website), on the Office's notice board and in the Office's internal telephone directory.

Any change in the person or contact details of the data protection officer must be communicated to the supervisory authority without delay.

The data protection officer shall be directly responsible to the notary public in his or her capacity as data protection officer and may only be instructed by the notary public in connection with this activity.

The work of the data protection officer in his or her other capacity shall be organised in such a way that the data protection officer is able to fully perform his or her tasks in his or her capacity as data protection officer in accordance with the provisions of the GDPR and these rules.

VIII/2. Tasks of the data protection officer

The data protection officer shall

a) continuously monitor changes in legislation relating to the processing of personal data, individual authority and court decisions and guidelines affecting the area of data protection law, and regularly inform the Office management and, if necessary, the Office staff;

b) provide professional advice and assistance to the Office staff in interpreting data protection legislation;

c) if necessary, in particular in the event of significant changes to national or European data protection legislation or the provisions of these rules, and in the event of significant changes in the powers and duties or organisational structure of the Office, provide information to the Office staff;

d) after prior consultation with the notary public, monitor compliance with the GDPR and other national and European legislation relating to the processing of personal data and the application of these rules;

e) where required by applicable national and European data protection legislation, make proposals to the notary public and the mayor to amend these rules, to issue or amend other regulations or instructions, and prepare drafts of the regulations or instructions to be issued or amended;

f) where necessary, make proposals to the notary public for the enactment or amendment of local government decrees;

g) ensure that these rules are continuously available to the Office staff and that any data protection information that may be necessary in individual cases is made available to data subjects;

h) provide professional advice on the data protection impact assessment and, if commissioned by the notary public, carry out the data protection impact assessment;

i) cooperate with the head of the Human Resources Group and the head of the IT Group to ensure full data protection and information security;

j) maintain and keep up to date the Office's data protection register;

k) cooperate with the supervisory authority;

l) in the event of a data breach, immediately report the data breach to the supervisory authority and make recommendations to the notary public and the head of the Office's organisational unit concerned by the data breach on the necessary measures to be taken;

m) prepare responses to data protection enquiries from data subjects;

n) prepare a report to the notary public by 28 February each year on his/her activities and experience as data protection officer in the previous calendar year, and formulate proposals for work organisation and internal regulation necessary for the effective implementation of national and European data protection legislation.

PART IX

FINAL PROVISIONS

IX/1. Data protection training

Employees are obliged to attend data protection training provided by the data protection officer within two months of the start of their employment relationship and every two years thereafter in order to familiarise themselves with the applicable national and EU data protection legislation and these rules. The training is organized by the data protection officer.

IX/2. Entry into force, publication

These rules shall enter into force on 1 August 2020. These rules shall be published on the Office's IT network, on the website www.bekescsaba.hu and on the Office's notice board.

Békéscsaba, 2020. július 27.

Szarvas Péter
polgármester

Dr. Bacsa Vendel
jegyző