JACZKOVICS
ÜGYVÉDI ▪ IRODA

PRIVACY POLICY

18 March 2024

WWW.JACZKOVICS.HU

TABLE OF CONTENTS

Based on 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 as "GDPR") as well as Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information (hereinafter as "Information Act"), Jaczkovics Law Office (hereinafter as "Office" or "Controller") has put in place the following policy to govern its rules concerning data protection, data security and data processing.

I. GENERAL PROVISIONS

1. The purpose and scope of effect of the Policy

1.1 The purpose of the Policy is to define the lawful regime of measures and procedures for the protection of personal data of natural persons processed by the Office in the course of its activities and operations, and to ensure the application of the fundamental principles of data protection, the right to informational self-determination, the right to the protection of personal data and the requirements of data security.

1.2 The personal scope of the Policy applies to any natural person working for the Office on the basis of an employment contract, membership, mandate or any other legal relationship for work, who process personal data in the course of their work.

The personal scope of the Policy also covers all natural persons who use the services or infrastructure of the Office, or who have or will have an actual contact with the Office, whether for the purpose of establishing a legal relationship or otherwise.

The personal scope of the Policy also extends to persons who do not have a legal or another relationship with the Office as described above, but whose personal data is processed by the Office based on a statutory obligation.

1.3 The material scope of the Policy covers personal data processed by the Office for any purpose and all records of personal data held by the Office, regardless of the form in which they are presented.

The scope of the Policy does not cover technical data protection related to IT equipment, which is covered by the IT and Information Security Policy.

2. Terms and Definitions used in the Policy

The terms used in this policy shall mean the following:

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. For the purposes of this Policy, all references to "data" are to personal data.

b) Sensitive data: data revealing racial or ethnic origin, nationality, political opinion or party affiliation, religious or other beliefs, membership of an interest representation organisation, personal data relating to sexual orientation, health status, harmful addictions, as well as criminal personal data.

c) Data processing: irrespective of the method applied, any operation or set of operations which is performed on personal data, in particular collection, obtaining, recording, organization, storage, alteration, use, query, transfer, disclosure, alignment or combination, restriction, erasure or destruction, and the prevention of further use of data, making photo, audio or video footage, and recording of physical attributes

suitable to identify a person (e.g. fingerprint or palm print, DNA sample, iris image), or access to such data.

d) Controller: the natural or legal person, public authority, or any entity without a legal personality who, independently, or jointly with others, determines the purposes for which the personal data is processed, makes and implements the decisions regarding the processing of the data (including the means applied) or ensures that they are implemented by processor.

e) Processor: means a natural or legal person, public authority, agency or other body which processes the personal data on behalf of the controller.

f) Third party: 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 authorised to process personal data.

g) Consent of the data subject: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.

h) Personal data breach: unlawful processing or handling of personal data, in particular unauthorised access, alteration, disclosure, transfer, disclosure, erasure or destruction, accidental destruction or accidental damage.

i) Data transfer: making data available to a specified third party.

j) Erasure: making the data unable to be identified so, that its recovery is not possible anymore.

k) Supervisory authority: the National Authority for Data Protection and Freedom of Information.

3. Controllers and data processing

3.1 Any person who has a legal relationship with the Office pursuant to Section 1.2 of this Policy and who obtains personal data or processes such data on the basis of their legal relationship with the Office shall protect and safeguard personal data and shall act in a manner that ensures their adequate protection.

3.2 Data must be protected against unauthorised access, alteration, transfer, public disclosure, erasure or destruction, as well as damage and accidental loss, and to ensure that stored data cannot be corrupted and rendered inaccessible due to any changes in or modification of the applied technique.

3.3 In the performance of their duties and the tasks arising from their contract, all persons in a legal relationship with the Office shall keep confidential any data, information or documents, accessed by them in whatever form and by whatever means, during the course of or in connection with the performance of their duties or the performance of their contract with the Office.

3.4 Persons who carry out controlling or processing operations while in a legal relationship with the Office shall be liable for any damage resulting from a breach of their data processing or data protection obligations.

3.5 The Office may only use data processors who or which provide appropriate guarantees for the execution of the appropriate technical and organizational measures ensuring compliance with data processing requirements and the protection of the rights of the data subjects.

3.6 Processing by a processor shall be governed by a contract or other legal act that is binding on the processor with regard to the Office and that sets out the subject-matter, the duration,

the nature and the purpose of processing, the type of personal data and the categories of data subjects and the rights and obligations of the controller. The contract must be concluded in writing and must include the content detailed in Article 28(3) of the GDPR, in particular, that the processor shall:

a) process personal data only on the basis of written instructions from the controller—including the transfer of personal data to a third country or an international organisation—unless the processing is required by Union or Member State law applicable to the data processor, in which case the data processor shall notify the controller of that legal requirement prior to processing unless the notification of the controller is prohibited by the relevant legislation on grounds of important public interest;

b) ensures that persons authorised to process personal data are bound by an obligation of confidentiality or are under an appropriate obligation of confidentiality based on law;

c) take the necessary measures to ensure the security of processing, as required in Article 32 of the GDPR;

d) respects the conditions referred to in Article 28(2) and (4) of the GDPR concerning the use of an additional data processor;

e) assist the data controller, to the extent possible, by appropriate technical and organizational measures, taking into account the nature of the processing, in fulfilling its obligation to respond to requests relating to the exercise of the data subject's rights under chapter III of the GDPR;

f) assists the controller in fulfilling its obligations under Articles 32 to 36 of the GDPR – in particular, reporting data breaches, conducting data protection impact assessment and preliminary consultation –, taking into account the nature of the processing and the information available to the data processor;

g) erase or return at the controller's discretion to the controller all personal data and delete existing copies after the provision of the processing service unless EU or Member State law requires the storage of personal data;

h) provide the controller with all the information necessary to demonstrate compliance with the obligations laid down above and to enable and facilitate audits, including on-site inspections, carried out by the controller or by another auditor assigned by the controller. The processor shall immediately inform the controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

3.7 Any company that is interested in the business activity for which personal data is used may not be contracted for the processing of such data.

3.8 Where necessary, the Office and the processor shall take further steps to ensure that any natural person acting under the authority of the Office or the processor who has access to personal data does not process such data except in compliance with the instructions from the controller, unless they are required to do so by European Union or Member State law.

4. The consent of the data subject as the legal basis for the data processing

4.1 Where processing is based on the consent of the data subject, the Office shall be able to demonstrate that the data subject has adequately consented to the processing of their personal data.

4.2 The consent of the data subject shall be considered a valid basis for processing where it is freely given, specific, informed and an unambiguous indication of the data subject's wishes

by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them. Remaining silent, a previously ticked box or inaction does not constitute consent.

4.3 The data subject's consent must ensure that they are given a real choice. Consent shall not be deemed to have been given voluntarily where the data subject does not have the possibility to refuse or withdraw consent without it being to their detriment, furthermore, where there is a clearly unequal relationship between the data subject and the controller.

4.4 Consent is not considered voluntary if it does not allow for separate consent for different personal data processing operations.

4.5 Consent is not considered voluntary, if performance of the contract (such as the provision of a service) is contingent upon consent to a processing operation that is not necessary for the performance of the contract.

4.6 The Office must provide an opportunity for the data subject to withdraw their consent at any time. The withdrawal of the consent does not affect the lawfulness of processing based on consent in the period prior to the withdrawal. Prior to giving consent, the data subject shall be informed thereof. It should be possible to withdraw consent in the same simple way as it is given.

4.7 If the Office obtains the data subject's consent through a written statement, the request for consent must be clearly and unambiguously separated from the rest of the contract and the request must be drafted in a clear and plain language by the controller.

5. Rights of data subjects and enforcement of these rights

5.1 Information obligation

5.1.1 Where the personal data processed are obtained by the Office from the data subject, the data subjects shall be informed, at the time of obtaining the personal data, in particular, of the identity and contact details of the controller and their representative, the purposes and legal basis of the intended processing of the personal data, the legitimate interest of the controller or of a third party in the event of processing based on legitimate interest, the recipients or categories of recipients of the personal data, the transfer to a third country or an international organization, the duration of storage of the data or the criteria for determining the duration, the right of the data subject to obtain from the Office access to the personal data relating to them, the rectification, erasure, restriction of the processing of such data, and they may object to the processing of such personal data, as well as the right of the data subject to data portability, the right to lodge a complaint with a supervisory authority, the fact whether the provision of the personal data is based on a legal or contractual obligation or is a precondition for the conclusion of a contract, and whether the data subject is under an obligation to provide the personal data and the possible consequences of not providing the data, and, where applicable, the existence of automated decision-making and profiling. Information on the possibility of enforcing the right of objection should be presented clearly and separately from any other information.

5.1.2 The above information must be provided

a) to persons who enter into an employment contract, agency contract, or another legal relationship for the performance of work, with the Office at the time the legal relationship is established, as part of the general information;

b) to persons who use the services of the Office on the basis of a contractual relationship, in accordance with the content of the relevant privacy notice of the Office

.

Information under clause a) must be provided on paper, in an electronic form or incorporated into the text of the contract, while information under clause b) must be provided by way of a reference in the contract to access to the related privacy notice.

5.1.3 If the personal data processed are not obtained by the Office from the data subject, the Office shall provide the data subject with the necessary information within a reasonable period of time from the acquisition of the personal data, but not later than one month, if the personal data are used for the purpose of communicating with the data subject, at least at the time of the first communication with the data subject, or, if the data are likely to be communicated to another recipients, at the latest at the time of the first communication of the personal data. As part of this, the data subjects must be informed, in particular, of the identity and contact details of the Office and its representative, the purposes for which the personal data are intended to be processed, the legal basis for the processing, the categories of personal data concerned, the recipients of the personal data and the categories of recipients, the fact whether data will be transferred to a recipient in a third country or to an international organization, the duration of the storage of the personal data or, if this is not possible, the criteria for determining this duration, the legitimate interests of the controller or of a third party where processing is based on legitimate interests, the right of the data subject to obtain from the Office access to, rectification, erasure, restriction of the processing of the personal data processed in relation to them, and they may object to the processing of such personal data, as well as the data subject's right to data portability and, where processing is based on consent, the data subject's right to withdraw their consent at any time, without prejudice to the lawfulness of processing carried out on the basis of consent prior to such withdrawal, the right to lodge a complaint with a supervisory authority, the source of the personal data and, where applicable, whether the data originate from publicly available sources, the existence of automated decision-making or profiling, where applicable.

5.1.4 The Office publishes the information related to its other activities involving the processing of personal data, which are not set out above – in order to make them available to the data subjects in advance – on its website under a dedicated tab "Data Protection" in a concise, transparent, intelligible and easily accessible form, in a clear and plain language.

5.1.5 In the case of a person whose mother tongue is not Hungarian, the information must also be provided in the mother tongue of that person. In such cases, the Office will arrange for the translation of the information.

5.1.6 The Office shall inform each recipient to whom the personal data have been disclosed about all cases of rectification, erasure or restriction of processing concerning the personal data unless it proves impossible or involves disproportionate effort.

5.2 Right to access

5.2.1 At the request of the data subject – accepted after the verification of their right – the Office shall, immediately upon receipt of the request, but no later than within 1 month, provide information about ongoing processing concerning the data subject, with the understanding that this deadline may not be extended.

5.2.2 The data subject may obtain access to the personal data and the following information:

a) the purposes of data processing;

b) the affected personal data categories;

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

d) where applicable, the planned duration of the storage of the personal data, or if this is not possible, the criteria based on which this duration is determined;

e) the data subject’s right to request the controller to rectify, erase or restrict the

processing of their personal data and to object to the processing of such personal data;

f) the right to file a complaint addressed to any supervisory authority;

g) if the data are not collected from the data subject, any and all information pertaining to the sources of such data;

h) the existence of automated individual decision-making, including profiling, or at least in these cases meaningful information on the logic applied and the significance of the processing and the envisaged consequences of such processing for the data subject.

5.2.3 Access to personal data must be provided in a manner that the data subject does not have access to personal data of other persons.

5.2.4 The data subject's right of access may be limited or refused by the Office in proportion to the aim pursued, if such a measure is strictly necessary to ensure that:

a) investigations or proceedings involving the Office, in particular criminal proceedings, are conducted effectively and successfully;

b) criminal offenses are prevented and detected effectively and successfully;

c) penalties and measures against offenders are enforced;

d) public safety is protected effectively and successfully;

e) the external and internal security of the State, in particular, national defense and national security, are protected effectively and successfully; or

f) the fundamental rights of third parties are protected.

5.2.5 If the Office refuses or restricts the right of access of the data subject, it shall immediately inform the data subject of this fact in writing – if this does not jeopardizes the purpose of the restriction or refusal – stating the reasons for the measure. In the information, the Office specifically draws the attention of the data subject to the fact that they may exercise their right of access with the assistance of the supervisory authority.

5.3 Right to rectification

At the request of the data subject – accepted after their right has been verified –, the Office will promptly take steps to rectify inaccurate personal data concerning the data subject. Taking into account the purposes of the processing, the data subject shall also have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

5.4 Right to blocking (restriction of processing)

5.4.1 At the request of the data subject – accepted after their right has been verified –, the Office shall restrict processing where one of the following conditions applies:

a) the data subject contests the accuracy of the personal data, in which case the restriction applies for the period of time necessary to allow the Office to verify the accuracy of the personal data;

b) the data processing is unlawful and the data subject opposes the erasure of the data and instead requests the restriction of their use;

c) the Office no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

d) the data subject has exercised their right to object to the processing. In this case, the restriction applies for the period until it is established whether the legitimate grounds

of the Office override those of the data subject.

5.4.2 Where processing is subject to the above restriction, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

5.4.3 A data subject who has obtained restriction of processing shall be informed by the Office before the restriction of processing is lifted.

5.5 Right to erasure

5.5.1 At the request of the data subject – accepted after their right has been verified –, the Office will promptly take steps to erase the personal data of the data subject, or the scope of personal data indicated by the data subject, provided that any of the following cases applies:

a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed by the Office;

b) the data subject withdraws the consent on which the data processing is based and there is no other legal basis for the data processing;

c) the data subject objects to the data processing and there are no overriding legitimate grounds for the data processing;

d) the processing of the personal data was unlawful;

e) the personal data must be erased in order to comply with a legal obligation under Union or Member State law to which the Office is subject.

5.5.2 If the Office has disclosed the personal data and is obliged to erase it in accordance with the above, the Office will take reasonable steps—including technical measures—, taking into account the available technology and the cost of implementation, in order to delete the links leading to the personal data or the copies or counterparts of the personal data.

5.5.3 The Office may not erase personal data despite a legitimate request if the processing is necessary for a purpose specified in Article 17(3) of the GDPR.

5.6 Right to object

5.6.1 Where the data subject's data are processed by the Office to enforce the legitimate interests of the Office or a third party, the data subject may object to the processing of such personal data, including profiling based on the aforementioned provisions. In this case, the Office may no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests or rights of the data subject or for the establishment, exercise or defence of legal claims.

5.6.2 Where personal data are processed for direct marketing purposes, the data subject has the right to object at any time to the processing of personal data concerning them for such purposes, including profiling. In case of such objection, the personal data shall no longer be processed for such purposes.

5.7 Right to remedy

If the data subject considers that the Office has infringed upon the applicable data protection requirements during the processing of their personal data, they may also contact the Office directly, which will investigate the complaint and, if justified, take the necessary measures, otherwise the complaint will be rejected. The Office shall inform the complainant in writing of the rejection of the complaint within 1 month of the receipt of the request at the latest,

stating the factual and legal reasons for the rejection. In cases where the request is denied, the Office shall inform the complainant of the judicial remedies available and the possibility of appealing to the authority. The Office shall prepare a record of the requests denied.

6. Security of data processing

6.1 In order to ensure data security, the Office shall assess and record all data processing activities it carries out.

6.2 On the basis of the records of processing activities, the Office will carry out a risk analysis to assess which organizational unit carries out which data processing operation and under what conditions, and which risk factors may cause damage and to what extent or what kind of potential personal data breach. The risk analysis should be based on the actual data processing activity that takes place. The purpose of the risk analysis is to determine security rules and measures that will ensure an adequate level of protection of the personal data in alignment with the operation and activities of the Office.

6.3 The Office shall implement appropriate technical and organisational measures to ensure and demonstrate that the processing of personal data is carried out in accordance with the GDPR—taking into account the nature, scope, context and purposes of the processing and the varying degrees of probability and severity of the risk to the rights of natural persons—, including, among other things, where appropriate:

a) the pseudonymisation and encryption of personal data;

b) the continuous confidentiality, integrity, availability and resilience of the systems and services used for personal data processing; the ability to restore access to and availability of personal data in the event of a physical or technical incident in a timely manner;

c) a procedure to regularly test, assess and evaluate the effectiveness of the technical and organisational measures taken to ensure the security of processing.

6.4 In determining the measures to ensure security of processing, the Office shall proceed taking into account the latest technical development and the state of the art of their implementation. Where alternate data processing solutions are available, the one selected shall ensure the highest level of protection of personal data, except if this would entail unreasonable hardship for the Office.

6.5 In determining the appropriate level of security, explicit account should be taken of the risks arising from the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transferred, stored or otherwise processed.

6.6 The Office shall implement appropriate technical and organisational measures to ensure that, by default, only personal data that are necessary for the specific purpose of the processing are processed. This obligation relates to the amount of personal data collected, the extent to which they are processed, the duration of their storage and their availability. These measures should in particular ensure that personal data cannot, by default, be made available to an indeterminate number of persons without the intervention of the natural person.

6.7 A document containing personal data must not be left in a place where it can be accessed by a third party. Such documents must also be locked away in office premises where third parties other than relevant staff members may be present.

6.8 To prevent the loss of manually processed personal data, original documents should only be released in the course of official business, in particular, in judicial proceedings or investigative procedures. Before their release, the original document must be copied in full for safekeeping at the Office.

6.9 The Office uses an electronic data management system that registers access to the system and it allows the identification of the person who recorded the data as well as the time and the date the data was recorded at.

6.10 In the event of damage or destruction of personal data, attempts should be made to replace the damaged data as far as possible from other available data sources. The fact that the data have been replaced shall be indicated in the data.

7. Data protection duties of the managing attorney

The managing attorney is responsible for the operation of the Office's data protection system, and all persons working for the Office on the basis of an employment contract, membership, a mandate or another legal relationship for the purpose of work must support his work and cooperate with him. These persons must perform their tasks with due regard for the risks associated with data processing operations and the nature, scope, context and purposes of the data processing.

8. Registries

The Office keeps electronic records:

a) the data processing activities performed at the Office. The records contains, in particular, the name and contact details of the Office, the name and contact details of the joint controller in the case of joint data processing, the purposes of the processing; the categories of data subjects and the categories of personal data; the categories of recipients to whom the personal data are or will be disclosed, where applicable, information on the transfer of personal data to a third country or an international organization (including a description of appropriate safeguards), if possible, the time limits envisaged for the erasure of the different categories of data; and, if possible, a general description of the technical and organizational security measures for data protection. The register should be continuously updated using the m_adatkezelesi_tevekenysegek_nyilvantartas template.

b) about personal data breaches detected at the Office. The register contains the scope of the personal data concerned, the scope and number of data subjects affected by the personal data breach, the date and time, circumstances and effects of the personal data breach and the measures taken to remedy it, as well as other data specified in the legislation providing for data processing, in accordance with the data content of the template m_adatvedelmi_incidens_nyilvántartas, for the purpose of monitoring the measures taken in relation to the personal data breach and informing the data subjects.

c) the data transfer performed at the Office. For the purposes of monitoring the lawfulness of the data transfer and informing the data subjects, the data transfer register contains the date and time of the data transfer of the personal data processed, the legal basis and the recipient of the data transfer, the scope of the personal data transferred and other data specified in the legislation providing for the data processing, as specified in the template named m_adattovabbitasi_nyilvantartas.

9. Privacy impact assessment

Having regard to preamble (91) of the GDPR, the Office does not carry out a data protection impact assessment.

10. Personal data breach management

10.1 If a controller acting on behalf of the Office becomes aware of a personal data breach in the course of processing data on behalf of the Office, either by themselves or by another

employee, they must immediately notify the office manager by filling out the form m_adatvedelmi_incidens_bejelentolap.

10.2 The office manager or the employee appointed by them will immediately, but not later than 72 hours, report the personal data breach to the supervisory authority unless the personal data breach is unlikely to pose a risk to the rights of the natural persons. If the notification is not made within 72 hours, it shall be accompanied by the reasons justifying the delay.

10.3 The notification to the supervisory authority shall include at least the following:

a) a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) the name and contact details of the other contact point where more information can be obtained;

c) a description of the likely consequences of the personal data breach;

d) a description of the measures taken or proposed to be taken by the Office to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

e) If it is not possible to provide the information at the same time as the notification, it may be provided in parts at a later date without further undue delay.

10.4 The Office will record personal data breaches, indicating the facts related to the personal data breach, its effects and the actions taken to remedy it.

10.5 When the personal data breach is likely to result in a high risk to the rights of natural persons, the Office shall communicate the personal data breach to the data subject or data subjects without delay. The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the following information:

a) the name and contact details of the office manager or the contact person appointed by them for providing meaningful information about the breach;

b) describe the likely consequences of the personal data breach;

c) the measures taken or proposed to be taken by the Office to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10.6 The communication to the data subject shall not be required if any of the conditions set out in Article 34(3) of the GDPR are met.

10.7 Following the implementation of the measures taken in relation to the personal data breach, the Office will assess the effectiveness of the measures and, if necessary, carry out a new risk analysis of the data concerned.

11. Data transfer

11.1 The processing operations carried out at the Office for different purposes may only be combined for legitimate purposes where justified.

11.2 A request for the transfer of personal data processed by the Office may only be executed on the basis of a legal requirement or if the data subject has given their consent – after having been informed in detail – in a verifiable manner. In all other cases, the data transfer shall be refused.

11.3 In the case of data transfers abroad, the person implementing the data transfer must specifically verify that the conditions for data transfer abroad set out in the GDPR are met.

In this context, it should be assessed whether the data transfer is made in accordance with a legal basis set out in the GDPR and whether an adequate level of data protection is ensured by the receiving controller. Where the data transfer is to a Member State of the European Economic Area, the adequate level of protection of personal data need not be assessed.

11.4 Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if the conditions laid down in the GDPR are complied with both by the controller and processor, including for onward transfers of personal data from the third country or an international organization to another third country or to another international organization.

11.5 A transfer of personal data to a third country or an international organization may take place if the European Commission has determined, and published in the Official Journal of the European Union and on its website, that the third country, a territory or one or more specific sectors of the third country, or the international organization in question ensures an adequate level of protection (adequacy decision). No specific authorisation shall be required for such data transfers.

11.6 The Office is entitled to transfer personal data for statistical purposes only, in such a way that they cannot be linked to the data subject.

II. SPECIAL PROVISIONS

1. Electronic access control system

1.1 The electronic access control system used by the Office is designed to prevent unauthorized access to the property used by the Office and to prevent possible crimes against property. The electronic access control system is operated by the Office.

1.2 Persons engaged by the Office under an employment contract, membership, contract for service or another legal relationship for the purpose of work, whose place of work is the property used by the Office, are entitled to an access card.

1.3 The Office shall keep a register of the cards (hereinafter referred to as the "card register") in which it processes the following data in relation to the access cards:

a) credit card number,

b) card code,

c) name of cardholder.

1.4 In the event of a permanent absence of the user of the access card, the data will remain in the register even after the card has been returned, until the legal relationship of the person concerned expires.

2. Alarm system

2.1 The alarm system used by the Office is designed to prevent unauthorized access to the property used by the Office and to prevent possible crimes against property.

2.2 The following persons are entitled to an access code:

a) persons engaged by the Office under an employment contract, membership, contract for service or another legal relationship for the purpose of work, whose place of work is the property used by the Office;

b) persons with an employment contract or in another legal relationship for the purpose of work with another organization related to the operation and management of the Office, who work in the property used by the Office.

2.3 The Office keeps a register of the access codes, which includes the following data:

a) access code,

b) name of the person using the access code,

c) the definition of the area covered by the right of access.

3. Personal data processed manually

3.1 In determining the measures to ensure security of processing, the Office shall proceed taking into account the latest technical development and the state of the art of their implementation. Where alternate data processing solutions are available, the one selected shall ensure the highest level of protection of personal data, except if this would entail unreasonable hardship for the Office.

3.2 For the security of personal data processed manually, the following measures shall be applied in particular:

a) documents deposited in the archive must be kept in a locked, dry room equipped with a fire- and property protection equipment;

b) only the relevant administrators have access to documents in permanent active processing; personnel, payroll and employment files must be kept securely locked away,

c) the documents relating to the data processing operations carried out by the Office must be archived regularly, and the archived documents must be sorted and deposited in the archive in accordance with the Office's document management policy.

3.3 The rules of access to the rooms concerned and the keys to the cabinets are determined by the managing attorney.

4. Personal data processed electronically

4.1 If the Office processes personal data in an electronic system, which can only be accessed by an authorized person registered on an access list, the authorized person must log in to the system with an individual, secret password the protection of which the authorized person must ensure – also in order to avoid personal data breaches – and must log out of the system after the end of the processing. The individual password allocated to the authorized person can only be known by the IT staff responsible for the development and operation of the data management software if it is necessary for the performance of their tasks at the Office.

4.2 The computers used for data processing may not be left unattended in a state suitable for data entry or retrieval.

4.3 The Office can only use an electronic data management system that registers access to the system and allows the identification of the person who recorded the data as well as the time and the date the data was recorded at.

III. CLOSING PROVISIONS

1. This Policy shall be made permanently available to all staff of the Office.

2. This Policy shall be published on the website of the Office.

3. This Policy – which will enter into force on 18 March 2024 – has been adopted by the General Assembly of the Office and all other policies issued on the same subject are repealed.

4. A list of templates relating to this policy is set out in Annex 1.