PRIVACY AND DATA MANAGEMENT POLICY

The purpose of this Privacy and Data Management Policy (hereinafter referred to as **Policy**) is to inform the persons concerned of the Regulation (EU) 2016/679 of the European Parliament and of the Council on general data protection regulations (hereinafter referred to as **GDPR**) and the Act CXII of 2011 on the Right to Self-Determination of Information and Freedom of Information (hereinafter referred to as **IL**) and the principles under the article 5 of GDPR (legality, fair procedure, transparency, purpose, data protection, accuracy, limited storage, integrity, confidentiality, accountability) on the part of **Taylor Fotó** (**Sándor Szabó** photographer).

TABLE OF CONTENTS

I. SCOPE OF THE POLICY
1. PERSONS COVERED
2. OBJECTS COVERED
3. DURATION
II. MANAGEMENT OF SPECIAL PERSONAL DATA
III. LEGALITY OF DATA MANAGEMENT
IV. COMPLETION OF DATA MANAGEMENT
1. DATA MANAGEMENT REQUIRED FOR CONTRACTUAL OBLIGATIONS
2. DATA MANAGEMENT REQUIRED FOR LEGAL OBLIGATIONS
3. CONSENT-BASED DATA MANAGEMENT
3.1 Customer service activities in person, by phone, e-mail
3.2 Sending newsletter or marketing letter
3.3 Use of electronic questionnaire for feedback and evaluation
3.4 Presence and marketing on social media
3.5 Data Management related to banking data
3.6 Complaint handling
V. DATA MANAGEMENT APPLIED ON THE WEBSITE
VI. THE RANGE OF PERSONS ACCESSING THE DATA
VII. DATA MANAGEMENT FOR ANOTHER DATA CONTROLLER
VIII. DATA SECURITY MEASURES
IX. ACTION IN THE EVENT OF A PRIVACY INCIDENT
1. OBLIGATIONS REGARDING THE PREVENTION OF A PRIVACY INCIDENT
2. REPORTING THE PRIVACY INCIDENT TO THE SUPERVISORY AUTHORITY
3. INFORMING THE DATA SUBJECT ABOUT THE PRIVACY INCIDENT
X. RIGHTS OF THE DATA SUBJECT
1. GENERAL RULES OF PROCEDURE RELATED TO THE EXERCISE OF RIGHTS OF THE DATA SUBJECT
2. RIGHT OF THE DATA SUBJECT TO PRIOR INFORMATION
3. RIGHT OF THE DATA SUBJECT OF ACCESS
4. RIGHT OF THE DATA SUBJECT TO RECTIFICATION
5. RIGHT OF THE DATA SUBJECT TO CANCELLATION
6. RIGHT OF THE DATA SUBJECT TO RESTRICT DATA MANAGEMENT
7. RIGHT OF THE DATA SUBJECT TO DATA PORTABILITY
8. RIGHT OF THE DATA SUBJECT TO PROTEST
9. AUTOMATED DECISION MAKING IN INDIVIDUAL CASE
10. RESTRICTIONS
XI. ENFORCING THE RIGHTS OF THE DATA SUBJECT

I. SCOPE OF THE POLICY

1. PERSONS COVERED

An identified or identifiable natural person, hereinafter referred to as **Data Subject**, is the natural person, who can be identified directly or indirectly, in particular on the basis of one or more factors relating to an identifier such as a name, number, location, online identifier or physical, physiological, genetic, mental, economic, cultural or social identity of a natural person.

The natural or legal person who determines the purposes and means of the processing of personal data, independently or together with others, hereinafter referred to as **Data Controller**. For the purposes of this Policy, the Data Collector is **Sándor Szabó** photographer (address: 18 II/9 Móricz Zsigmond street, Ajka, 8400, Hungary; mother's name: dr. Mária Balogh; serial number of photographer certificate: CXB C 1303427; e-mail address: sandor.szabo@taylor-foto.hu; telephone number: +36 20 254 8999).

A natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller, hereinafter referred to as **Data Processor**. For the purpose of this Policy, the identity of the Data Controller and the Data Processor is the same, the Data Controller does not use any other Data Processor.

A natural or legal person, public authority, agency, or any other body that is not the same as the Data Subject, the Data Controller, the Data Processor or the persons who have been authorized to process personal data under the direct control of the Data Controller or the Data Processor, hereinafter referred to as **third party**.

2. OBJECTS COVERED

Any information about the Data Subject, hereinafter referred to as **Personal Data**.

Data referring to racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as data referring to unique identification of individuals by genetic or biometric data, health data and the sex life or sexual orientation of natural persons, hereinafter referred to as **Special Personal Data**.

In any of the operations performed upon personal data or files on an automated or non-automated means or the whole of operations, including, but not limited to the collection, recording, organization, division, store, reconstruction, alteration, consultation, use, disclosure, transmission, distribution, publication or otherwise make available, reconcile, link, restrict, delete or destroy, hereinafter referred to as **Data Management**.

A security breach that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Personal Data transmitted, stored or otherwise handled, hereinafter referred to as a **Privacy Incident**.

3. DURATION

This Policy is valid from 15 August 2020 until its revocation or the entry into newer Policy – by which this Policy and all previous Policies expire.

The Data Controller reserves the right to amend the Policy and publish a new Policy on its website. With the publication of the new Policy, the previous Policy will expire.

II. MANAGEMENT OF SPECIAL PERSONAL DATA

The Data Controller does not request or process Special Personal Data, except for certain data required by laws in the case of an employment relationship.

Special Personal Data brought to the knowledge of the Data Controller in any way shall not be recorded by the Data Controller. If such data has been entered into any system of the Data Controller without the knowledge of the Data Controller, it shall be deleted from its system immediately upon its detection.

III. LEGALITY OF DATA MANAGEMENT

The Data Controller and the Data Processor examine the lawfulness of Data Management at all stages of their activities, handling only data and for a period of time for which it can justify its purpose and legal basis. In the case of termination of the condition of the legal basis, the Data Management only be continued if the Data Controller can certify other appropriate legal basis.

The legal basis of the Data Management by the Data Controller and the Data Processor:

- the Data Management is necessary for the fulfillment of a contractual obligation concerning the Data Subject as a contractual party (point b) of subsection (1) of article 6 of GDPR);
- the Data Management is necessary to fulfill a legal obligation on the Data Controller (point c) of subsection (1) of article 6 of GDPR);
- the Data Management is necessary to enforce the legitimate interests of the Data Controller (point f) subsection (1) of article 6 of GDPR);
- the Data Subject has given its consent to the processing of Personal Data (point a) of subsection (1) of article 6 of GDPR).

As a general rule, the method of justifying legal basis is in writing. The legal basis established by oral or implied behavior must be examined whether it clearly be justified subsequently. In case of doubt, for reasons of reasonableness and economy, efforts should be made to confirm in writing the legal basis for the oral or implied behavior.

In connection with the contractor of an existing valid contract, the Data Controller shall continue to process the data of the contractor, after the entry into force of the GDPR, until the termination of the contract in accordance with point b) of subsection (1) of article 6 of GDPR.

Following the termination of the contract, the Data Controller shall perform Data Management in order to enforce the legal obligation applicable to it or the legitimate interest of the Data Controller, until its verifiable existence.

IV. COMPLETION OF DATA MANAGEMENT

1. DATA MANAGEMENT REQUIRED FOR CONTRACTUAL OBLIGATIONS

The purpose of the Data Management is to provide the Data Subject with appropriate information and support, as well as to ensure contact in order to prepare, conclude, maintain, perform and terminate the contract, and to enforce the rights of the Data Controller arising from the contractual relationship.

The legal basis for the Data Management is the fulfillment of the obligations arising from the contract between the parties, in accordance with point b) of subsection (1) of article 6 of GDPR.

The recipients of the Personal Data are the Data Controller and its employees, and if the Data Subject is a legal person, the employees of the Data Subject, who act in order to prepare, conclude and perform the contract.

For the purposes of Data Management, a Data Subject is any natural person, who acts in its own name or as a representative, agent or contact person of a legal entity when requesting information, requesting a quote or concluding a contract.

Scope and purpose of the data processed:

- When requesting information or requesting a quote by a natural person, for identification purposes: the name of the natural person.
- When requesting information or requesting a quote by a legal person, for identification purposes: the name of the legal person and the name of the natural person acting on behalf of the legal entity.
- When concluding contract with a natural person, for identification purposes: name, date and place of birth, address of residence, name of mother, and number of identity card of the natural person.
- When concluding contract with a legal person, for identification purposes: name, registration number, and registered office of the legal person, as well as name, date and place of birth, address of residence, name of mother, and number of identity card of the representative.
- In case of legal and natural person, for contact purposes: e-mail address or telephone number of the contacting natural person.

The duration of the Data Management is the period of validity of the offer or contract, or after its termination, until the expiry of the rights arising from the contract in the legitimate interest of the Data Controller, and the expiry of the retention period according to the accounting rules. In the case of a business relationship with a legal person, the duration of the Data Management is up to five (i.e. 5) years after the termination of the business relationship, if the limitation period for the rights arising from the legitimate interest of the Data Controller is shorter.

2. DATA MANAGEMENT REQUIRED FOR LEGAL OBLIGATIONS

The purpose of the Data Management is to process documents containing Personal Data of natural and legal persons and their representatives (including but not limited to invoices, delivery notes), who came in contract with the Data Controller as customer or supplier, on the basis of the related laws in force. Such provisions, in particular, the section 50 of the Act CL of 2017 on the Order of Taxation, the section 169 of the Act CXXVII of 2007 on the Value Added Tax, and the section 167 of the Act C of 2000 on the Accounting.

The legal basis of the Data Management is the fulfillment of the legal obligation to the Data Controller.

The recipients of the Personal Data are the Data Controller and its employees, who performing the tax and accounting administration, and the Data Processors and its employees, who providing such services, as well as the manager of the payment order of the employer, and the Data Processor and its employee, who inspecting the above.

For the purposes of Data Management, a Data Subject is any customer and supplier, who comes in contact with the Data Controller in that capacity.

Scope and purpose of the data processed is the data content required by the laws and the data of the documents used to fulfill the legal obligations.

The duration of the Data Management is the eight (i.e. 8) years period following the financial transaction taken.

3. CONSENT-BASED DATA MANAGEMENT

3.1 Customer service activities in person, by phone, by e-mail

The Data Controller performs customer service activities in person, by phone or by e-mail. If the Data Subject receives an appropriate service in person or by phone in connection with all the issues, and the Personal Data of the Data Subject are not recorded, then the Data Management will not take place. If the service can only be implemented by recalling the Data Subject or sending information by e-mail, and the data provided by the Data Subject is recorded by the Data Controller in a paper-based call log or on an electronic interface (hereinafter referred to as Call Log), then the Data Management is performed by the Data Controller as follows.

The purpose of the Data Management is to fulfill information service to the Data Subject by phone or by e-mail.

The legal basis of the Data Management is the consent of the Data Subject. Consent shall be deemed to have been given if the Data Subject dictates its contact details to the Data Controller by itself, or if it contacts the Data Controller by e-mail.

The recipients of the Personal Data are the Data Controller and its employees, who deal with the transmission of information.

For the purposes of Data Management, a Data Subject is any natural person, who contacting the Data Controller or its employees performing customer service activities, by phone or by e-mail.

Scope and purpose of the data processed is the name of the Data Subject and the time of contact, for identification purposes, as well as the telephone number or e-mail address of the Data Subject, for contact purposes.

The duration of the Data Management is the three (i.e. 3) months period from the date of the response.

3.2 Sending newsletter or marketing letter

The purpose of the Data Management is to perform Data Management in connection with sending newsletter or marketing letter. The purpose of the newsletter and the marketing letter is transmission of complete, general or personalized information, about the promotions, discounts, events and news displayed on the website of the Data Controller, and providing information on changes and lags of notification services, in accordance to the relevant and applicable laws. Such provisions, in particular, the section 6 of Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions of Commercial Advertising.

The legal basis of the Data Management is voluntary subscription and contribution for sending a newsletter or a marketing letter.

The recipients of the Personal Data are the Data Controller and its employees, who provide customer service and marketing activities, and the Data Processors and its employees, who provide IT services, newsletter sending services or hosting services.

For the purposes of Data Management, a Data Subject is any natural person, who whish to be informed about the news, promotions or discounts of the Data Controller on a regular basis, and who sing up for newsletter or marketing letter service. Confirming signing up can be done via not pre-checked checkbox or button.

Scope and purpose of the data processed is the name of the Data Subject, for identification purposes, and the e-mail address of the Data Subject, for purpose of sending e-mail.

The duration of the Data Management is the period, from the beginning of the subscription of the Data Subject until the termination request (un-subscription) of the Data Subject, or until the termination of the newsletter or marketing letter service.

The Data Subject may unsubscribe from the newsletter or marketing letter at any time, via the "Unsubscribe" link at the bottom of the e-mails (hereinafter referred to as Immediate Unsubscribe); or by sending an e-mail with "Unsubscribe" subject to taylor-foto@taylor-foto.hu, stating that is requests the cancellation of the newsletter or marketing letter service; or by post to Taylor Fotó (Sándor Szabó), 7 V/2 Galamb street, Budapest, 1052, Hungary with the same content as unsubscribing by e-mail.

The Data Subject wishing to unsubscribe should be aware, with the exception of Immediate Unsubscribe, that the un-subscription may have a lead time of a few days, during which the system may send further newsletter or marketing letter to the Data Subject, which does not mean breach of the provisions of the Data Management included in this Policy.

The Data Controller draws the attention of the Data Subject, that the newsletter or marketing letter sent at the same or nearly the same time as an Immediate Unsubscribe may avoid each other for technical reasons, therefore newsletter or marketing letter received after the un-subscription is not consider as failure of the un-subscription request.

3.3 Use of electronic questionnaire for feedback and evaluation

The purpose of the Data Management is to measure and improve the quality of the service and to keep in touch with the Data Subject, in case the feedback or evaluation is not anonymous.

The legal basis of the Data Management is voluntary fill of the feedback or evaluation questionnaire. In case of anonymous feedback, when the person providing the assessment cannot be identified, no Data Management will take place.

The recipients of the Personal Data are the Data Controller and its employees, who process the feedback or evaluation, and the Data Processors and its employees, who perform IT services or hosting services.

For the purposes of Data Management, a Data Subject is any natural person, who has been a recipient of the service of the Data Controller and gives an assessment in response to a call for feedback or evaluation.

Scope and purpose of the data processed is the name of the Data Subject, for identification purpose, the e-mail address or telephone number of the Data Subject, for contact purposes, and the name and evaluation of the service used, in order to achieve the Data Management purpose.

The duration of the Data Management is the time until achieving the purpose.

3.4 Presence and marketing on social media

The purpose of the Data Management is to share content from the website of Data Controller on social sites, as well as to draw attention to this, and marketing purposes.

The legal basis of the Data Management is the voluntary consent of the Data Subjects related to the profile of the Data Controller on the social sites.

The recipients of the Personal Data are the Data Controller and its employees, who support the community presence and marketing of the Data Controller, and the Data Processors and its employees, who provide IT services and hosting services.

For the purposes of Data Management, a Data Subject is any natural person, who visit, follow, value the content (like, dislike), comment, share partly or fully the social sites of the Data Controller.

Scope and purpose of the data processed is the name and photo (profile picture) of the Data Subject, for identification purposes, posts, comment, evaluation, express of mood, content of question or request, in order to achieve the Data Management purpose.

The duration of the Data Management is the period until the end of the public availability of the data published by the Data Subject and the social sites, and until the operation of the social sites of the Data Controller.

Personal Data published by the visitors on the social sites of the Data Controller is not managed by the Data Controller. In case of any illegal or offensive content, the Data Controller has the right to delete the given content. Further information on the use of social sites of the Data Controller is available at the following locations:

- Facebook: https://www.facebook.com/legal/terms
- Instagram: https://help.instagram.com/581066165581870
- Bēhance: https://www.adobe.com/legal/terms.html
- LinkedIn: https://www.linkedin.com/legal/user-agreement

3.5 Data Management related to banking data

The purpose of the Data Management is to facilitate the financial performance of the Data Subject.

The legal basis of the Data Management is the voluntary provision of data related to bank transfers.

The recipients of the Personal Data are the Data Controller and its employees, who deal with accounting tasks, as well as the Data Processors and its employees, who provide accounting services.

For the purposes of Data Management, a Data Subject is any natural and legal person, who wish to pay by bank transfer.

Scope and purpose of the data processed is the name, bank account number of the Data Subject (account holder), the message of the transfer, for identification purposes, the e-mail address or postal address of the Data Subject, in order to send the payment request and the invoice, the transfer amount, in order to fulfill the transfer.

The duration of the Data Management is the corresponding period according to the valid accounting rules.

3.6 Complaint handling

The purpose of the Data Management is to enable the communication of the complaint, to identify the Data Subject and its complaint, as well as to record the data that must be recorded in accordance with the laws, and to ensure the communication during investigation and settlement of the complaint.

The legal basis of the Data Management is the voluntary submission of the complaint, however, in the case of the complaint made, the mandatory provisions of the Act CLV of 1997 on the Consumer Protection (hereinafter referred to as CP).

The recipients of the Personal Data are the Data Controller and its employees, who deal with complaints.

For the purposes of Data Management, a Data Subject is any natural person, who wish to place complaint related to ordered or fulfilled service, as well as who wish to communicate its complaint orally or in writing, related to the behavior, activity or failure of the Data Controller.

Scope and purpose of the data processed is the ID of the complaint, time of receipt, name of the Data Subject, for identification purposes, e-mail address or telephone number of the Data Subject, for contact purposes, name of the service or the behavior complained, reason, related documents of the complaint, for investigating purposes.

The duration of the Data Management is the period of five (i.e. 5) years in accordance with the provisions of the subsection (7) of section 17/A of CP.

The Data Subject can file a complaint to the Data Controller by sending e-mail to the taylor-foto@taylor-foto.hu e-mail address with "Complaint" subject, which contains the relevant information related to the complaint; or by post to Taylor Fotó (Sándor Szabó), 7 V/2 Galamb street, Budapest, 1052, Hungary with the same content as sending complaint by e-mail.

The Data Controller is obliged to keep a record of a personal oral complaint.

In accordance with the provisions of the CP, the Data Controller shall respond to the written complaint and take action on its communication within thirty (i.e. 30) days after receipt of the complaint, or if a shorter deadline is established by laws, until its expiry. The Data Controller is obliged to justify its position rejecting the complaint.

V. DATA MANAGEMENT APPLIED ON THE WEBSITE

It is possible to view the content accessible to anyone published on the website of the Data Controller without providing Personal Data. The website automatically records the following information about visitors: IP address of the visitor, the time of the visit, the pages and content viewed on the website. This data is used by the Data Controller only for the analysis of the website and for checking the secure operation of the website.

The website operates so-called "cookies", which store information about the use of the website. The purpose of managing the data stored in cookies is to increase the user experience and improve the online services of the website. The cookies used on the website do not store personally identifiable information.

When visiting the website, the user may remove the cookies placed by the website from its own computer at any time or disable the use of the cookies in its browser.

VI. THE RANGE OF PERSONS ACCESSING THE DATA

The Data Controller and the Data Processor may access the Personal Data provided by the Data Subject in order to fulfill their functions. The processing of Personal Data is basically carried out by the Data Controller, or in connection with the individual outsourced activities by the Data Processors. In this case the Data Controller transfers data to the Data Processors, or they may have access to data due to the nature of their activities. The Data Controller is responsible for the activities of the Data Processors.

The legal representative representing the Data Controller may also acquire the Personal Data of the Data Subject if legal proceedings are initiated on the basis of the submission of the Data Subject.

The Data Controller shall transfer the Personal Data of the Data Subject to other public bodies only in the following exceptional cases:

- If the Data Controller transfers the case containing the Personal Data of the Data Subject to the Archives in accordance with the legislation on archiving and its own internal regulations.
- If a court case is initiated in a case related to the Data Subject and it is necessary for the trial court to hand over the documents containing the Personal Data of the data Subject.
- If the investigating authority contacts the Data Controller and requests the transmission of documents containing the Personal Data of the Data Subject for the ongoing investigation.

VII. DATA MANAGEMENT FOR ANOTHER DATA CONTROLLER

According to the rules of the contract concluded with the third party, the Data Controller (hereinafter referred to as Agent) may perform data processing activities for other Data Controller.

In respect of the above, as provided for in article 28 of GDPR, the Agent warrants that

- the Data Management carried out for the other Data Controller in according to the requirements of the GDPR shall be performed by implementing appropriate technical and organizational measures to ensure the protection of rights of the Data Subject;
- does not use an additional Data Processor without the prior written ad hoc or general authorization of the other Data Controller;
- if the additional Data Processor used with the authorization of the other Data Controller failed to fulfill its data protection obligations, the Agent shall be fully liable to the other Data Controller for the fulfilment of the obligations of the additional Data Processor.

The Agent in accordance with the rules of the contract concluded between the parties

- processes Personal Data only on the basis of written instructions of the other Data Controller;
- ensures that persons authorized to process data are bound by an obligation of confidentiality or are subject to an appropriate obligation of confidentiality by laws;
- implements appropriate technical and organizational measures in accordance with the security provisions of the GDPR in order to guarantee the appropriate level of data security commensurate with the degree of risk. Such measures shall include, in particular, the pseudonymisation and encryption of Personal Data, the continued confidentiality of systems and services used to process Personal Data, their integrity, availability and resilience, and the ability to access Personal Data in a timely manner in case of the event of a physical or technical incident in a timely manner, and the application of procedures for regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures taken to ensure the security of Data Management.
- takes appropriate technical and organizational measures to assist the other Data Controller, as far as possible, in fulfilling its obligation to respond to requests relating to the exercise of rights of the Data Subject.
- in the event of a Privacy Incident relating the other Data Controller, the Agent shall notify the other Data Controller without undue delay after becoming aware of it and shall cooperate in mitigating the adverse consequences arising from the Privacy Incident;
- allows the other Data Controller to verify compliance with the obligations of the Agent, either in person or through another inspector or auditor appointed by the other Data Controller;
- upon termination of the provision of the service, the Data Controller shall, based on its own decision, delete or return all Personal Data to the other Data Controller and also delete existing copies, unless EU or Member State laws provide for the storage of Personal Data.

The Agent shall also enforce all data security measures and developments with its data processing activities performed for the other Data Controller, which introduced related to its own data processing activities.

VIII. DATA SECURITY MEASURES

The Data Controller stores the Personal Data provided by the Data Subject primarily on the servers of the Data Processor specified in this Policy equipped with standard protection systems, partly on its own IT devices, and in the case of paper data carriers at its registered office or premises, stored properly closed. For storing Personal Data, the Data Controller does not use services of other contributors.

The Data Controller shall take the necessary measures to ensure that the Personal Data is protected against unauthorized access or alteration and similar actions.

In order to secure access to data stored in digital form, in file, using cloud service, the Data Controller shall establish strong password protection that provides sufficient security and shall update it with sufficient frequency.

The Data Controller ensures that accesses to its system are logged and analyzes the log data on a regular basis. In the event of any indication of an anomaly, the Data Controller will take the necessary preventive or incident management measures.

The Data Controller ensures the binding of passwords to the users during the use of the devices and systems used, and regularly checks their proper use. These include, in particular, prohibiting the use of the same password by more than one user, storing passwords in a way that is inaccessible to others, making it technically impossible to disable password protection or, failing that, prohibiting it.

The Data Controller also uses the available password protection solutions of the digital documents in case of transferring digital documents to the Data Processor, thus ensuring that the data of the document cannot be accessed by an unauthorized person.

In the case of data stored on paper data carrier or in other analogous way, physical security must also be ensured by using lockable containers and guarding the keys securely.

During the performance of the activity, reasonable measures must be taken to ensure with the use of a cover or folder, the folding of the document or similar ways, that the data stored on the paper media are not made known to others.

At the end of the day-to-day activities, the Data Controller must allow sufficient time for the documents generated during the day to be kept in a locked place and not accessed by unauthorized persons. Compliance with this is regularly monitored by the Data Controller.

The Data Controller ensures with regular training, that the human factor necessary to establish and maintain data security is kept at a high level. Education should include maintaining a high level of user responsibility and making data security a part of everyday routine through the development of good practices. These may include, in particular, a laptop, telephone or document containing Personal Data may not be left in the car by the user or left unattended, and shall be locked in a safe in a hotel.

The user is obliged to report the slightest sign of abnormal operation to the Data Controller.

The Data Controller within the cooperation with the Data Processor shall mutually ensure that properly trained and authorized persons with knowledge of access data of each other are available to take data protection measures, to prevent Privacy incidents and to take effective mitigation measures in case of Privacy incidents.

IX. ACTION IN THE EVENT OF A PRIVACY INCIDENT

1. Obligations regarding the prevention of a Privacy Incident

The Privacy Incident (a security breach that results in the accidental or unlawful destruction, loss, alteration, unauthorized publication, or unauthorized access of the stored, transmitted or otherwise handled Personal Data) must be prevented in all reasonable and accessible ways.

When the Data Controller becomes aware of any signs of a Privacy Incident, it immediately investigates it and makes sure a Privacy Incident in fact occurred or not.

Even in the case that an event does not qualify as a Privacy Incident – if a conclusion can be drawn from it for the purpose of later safer operation – the event must be documented and the Data Controller will take the necessary measures on this basis.

2. Reporting the Privacy Incident to the supervisory authority

The Privacy Incident shall be reported by the Data Controller, without undue delay, if possible no later than seventy-two (i.e. 72) hours after becoming aware of the Privacy Incident, to the supervisory authority competent in accordance with the article 55 of the GDPR, unless the Privacy Incident is unlikely to pose risk to the rights and freedoms of natural persons. If the report is not made within seventy-two (i.e. 72) hours, the reasons for the delay must be attached.

The Data Processor shall report the Privacy Incident to the Data Controller, without undue delay, after becoming aware of it.

It must be described in the report on Privacy Incident

- the nature of the Privacy Incident, including, where possible, the categories and approximate number of Data Subjects and the categories and approximate number of data involved in the incident;
- the name and contact details of the data protection officer or other contact person, who can give further information;
- the likely consequences of the Privacy Incident;
- the measures taken or planned by the Data Controller to remedy the Privacy Incident, including, where appropriate, measures to mitigate any adverse consequences arising from the Privacy Incident.

If and where it is not possible to communicate the information at the same time, it may be communicated in detail at a later date without further undue delay.

The Data Controller shall keep a record of the Privacy Incidents, indicating the facts related to the Privacy Incident, its effects and the measures taken to remedy it. This record shall enable the supervisory authority to verify the compliance with the requirements.

3. Informing the Data Subject about the Privacy Incident

If the Privacy Incident is likely to pose a high risk to the rights and freedoms of natural persons, the Data Controller shall, without undue delay, inform the Data Subject about the Privacy Incident.

In the information on Privacy Incident must be clearly and intelligibly described

- the nature of the Privacy Incident, including, where possible, the categories and approximate number of Data Subjects, and the categories and approximate number of data involved in the incident;
- the name and contact details of the data protection officer or other contact person, who can give further information;
- the likely consequences of the Privacy Incident;
- the measures taken or planned by the Data Controller to remedy the Privacy Incident, including, where appropriate, measures to mitigate any adverse consequences arising from the Privacy Incident.

The Data Subject need not be informed if any of the following conditions are met:

- The Data Controller has implemented appropriate technical and organizational security measures and these measures have been applied to the data affected by the Privacy Incident, in particular those measures, which do not allow access to Personal Data by making the data meaningless to the unauthorized persons.
- Following the Privacy Incident, the Data Controller has taken measures to ensure that the high risk to the rights and freedoms of the Data Subject is unlikely to materialize.
- The information would require a disproportional effort. In such cases, Data Subjects shall be informed through publicly available information or a similar measure shall be taken to ensure that Data Subjects are informed in an equally effective manner.

If the Data Controller has not informed the Data Subject about the Privacy Incident, the supervisory authority, having considered that the Privacy Incident is likely to be high risk, orders to inform the Data Subject, or determines the filing exemption conditions met.

X. RIGHTS OF THE DATA SUBJECT

1. General rules of procedure related to the exercise of rights of the Data Subject

The Data Controller provides information about handling the Personal Data, and all other relevant information, with this Policy or based on it, and it strives to transfer it in solid, transparent, easy accessible, in a clear and understandable form. In the case of any extract, reference must be made to the full Policy document – attached or made available through a link.

The information relevant to the Data Subject can be given to the Data Subject only. Unless the person requesting the information can be identified as a person concerned beyond a reasonable doubt, the information shall be refused. A person acting on behalf of the Data Controller is obliged to draw up a report on such a case, with a precise recording of the facts, which can be a basic document in the handling of a possible complaint.

Identification shall also be carried out in accordance with the principles set out in article 5 of the GDPR (legality, fairness and transparency, purpose, data economy, accuracy, limited storage, integrity and confidentiality, accountability) and shall be carried out in accordance with the principles of necessity and sufficiency. Accordingly, no further identification is required in the event of a request from the e-mail address of the Data Subject managed by the Data Controller.

If the Data Subject has submitted its request by electronic means, the information shall, as far as possible, be provided by electronic means, unless the Data Subject requests otherwise.

The information can be given orally requested by the Data Subject, if it confirmed its identity correctly.

The Data Controller is obliged to inform the Data Subject of the measures taken following the request no later than within one (i.e. 1) month from the receipt of the request. If necessary, taking into account the complexity of

the application and the number of applications, this time limit may be extended by a further two (i.e. 2) months. The Data Controller shall inform the Data Subject of the extension of the time limit, indicating the reasons for the delay, within one (i.e. 1) month from the receipt of the request.

If the Data Controller does not take action on the request of the Data Subject, it shall without delay, but no later than within one (i.e. 1) month from the receipt of the request, and inform the Data Subject of the reasons for the non-action and that the Data Subject may file a complaint to a supervisory authority and may exercise its right of legal remedy.

The Data Controller shall inform all recipients to whom the Personal Data has been communicated of any rectification, erasure or restriction on data processing, unless this proves impossible or requires a disproportionate effort. In the request of the Data Subject the Data Controller informs the Data Subject about these recipients.

2. RIGHT OF THE DATA SUBJECT TO PRIOR INFORMATION

The Data Controller provide the Policy, which contains the information accordance with the article 13 and 14 of the GDPR, to the Data Subject, when the Data Controller get its Personal Data.

The Data Controller places the Policy to its website in downloadable form and also post it in a place accessible to all Data Subjects on paper.

3. RIGHT OF THE DATA SUBJECT OF ACCESS

The Data Subject may request in writing the Data Controller through the contact details of the Data Controller, to inform, whether it manages its Personal information or not, if so, then what kind of Personal Data and what purpose, to what recipients is communicated, how long the Data Controller plans to store it, if not all information was collected from the Data Subject, then all information of the source, whether it was transmitted to a third country or to an international organization, or not, if so, with what guarantees (article 46 of the GDPR).

The information shall also be accompanied by information on the rights of the Data Subject, to request the Data Controller to rectify, delete or restrict the processing of Personal Data, and to object to the processing of Personal Data, or to lodge a complaint with the supervisory authority.

The Data Controller makes available to the Data Subject the copy of the Personal Data issued. For further copies requested by the Data Subject, the Data Controller may charge a reasonable fee based on administrative costs. If the request has been submitted by the Data Subject by electronic means, the information shall be provided in a widely used electronic format, unless otherwise requested by the Data Subject. The right to request a copy must not adversely affect the rights and freedoms of others.

4. RIGHT OF THE DATA SUBJECT TO RECTIFICATION

The Data Subject is entitled to request the Data Controller to correct its Personal Data without undue delay. Taking into account the purpose of the Data Management, the Data Subject is entitled to request that the incomplete data be supplemented, inter alia, by means of a supplementary statement.

5. RIGHT OF THE DATA SUBJECT TO CANCELLATION

The Data Subject may request in writing the Data Controller through the contact details of the Data Controller to delete its Personal Data, if

- the Personal Data are no longer required for the purpose for which they were collected or otherwise processed;
- the Data Subject withdraws its consent to Data Management and there is no other legal basis for the Data Management;
- the Data Subject protests against Data Management pursuant to subsection (1) of article 21 of the GDPR and there is no overriding legitimate reason for Data Management, or the Data Subject protests against Data Management pursuant to subsection (2) of article 21 of the GDPR;
- the Personal Data were processed unlawfully;
- the Personal Data must be deleted in order to comply with a legal obligation under EU or Member State laws applicable to the Data Controller;
- the Personal Data were collected in connection with the provision of information society services referred to in subsection (1) of article 8 of the GDPR.

If the Data Controller published the Personal Data and it is required to be deleted, then the Data Controller will take into reasonable steps in accordance with the costs of the available technology and implementation – including the technical measures as well – in order to inform the Data Controllers, who manage the data, about the Data Subject requested the deletion of the links, copies or duplicates of the Personal Data.

The Data Controller may refuse the deletion if the Data Management is necessary for the submission, enforcement or protection of legal claims or in other cases pursuant to subsection (3) of article 17 of the GDPR.

6. Right of the Data Subject to restrict Data Management

The Data Subject is entitled to request the Data Controller to restrict Data Management, if

- the Data Subject disputes the accuracy of the Personal Data, in which case the restriction applies to the period of time that allows the Data Controller to verify the accuracy of the Personal Data;
- the Data Management is illegal, but the Data Subject oppose the deletion of the data, and instead of it requests for restrictions on their use;
- the Data Controller no longer needs the Personal Data for the purpose of Data Management, but the Data Subject requests it in order to submit, enforce or protect legal claims;
- the Data Subject protests against Data Management pursuant to subsection (1) of article 21 of the GDPR, in which case the restriction applies to the period of time that allows the Data Controller to establish, whether the legitimate reasons of the Data Controller take precedence over those of the Data Subject.

If the Data Management is restricted because of any reasons described above, then the Persona Data, in exception of storage, may only be dealt with the consent of the Data Subject, or for the submission, enforcement or protection of legal claims, or for protection of rights of other natural or legal person, or because of important public interest of the EU or of a Member State.

The Data Controller, at the request of the Data Subject, at whose request the Data Management has been restricted for one of the above reasons, shall inform in advance of the lifting of the restriction of the Data Management.

7. Right of the Data Subject to data portability

The Data Subject is entitled to receive the Personal Data concerning and provided by the Data Subject, in a structured, widely used machine-readable format, and to transfer such data to another Data Controller without hinder the Data Controller, who provided the Personal Data, if the Data Management is based on the consent of the Data Subject, or on a contract between the Data Subject and the Data Controller as contractual parties, or if the Data Management takes place in an automated manner.

In exercising the right to data portability, the Data Subject shall have the right, if technical feasible, to request the direct transfer of Personal Data between Data Controllers.

The exercise of the right to data portability shall not aggrieve the provisions of the GDPR concerning the right of erasure. This right shall not apply if the Data Management is necessary for the performance of a task in the public interest or in the exercise of public authority powers conferred on the Data Controller.

The right to data portability must not adversely affect the rights and freedoms of others.

8. Right of the Data Subject to protest

The Data subject is entitled to object at any time, for reasons relate to its situation, to the processing of its Personal Data on the basis of point e) or f) of subsection (1) of article 6 of the GDPR, including profiling based on those provisions. In this case, the Data Controller may not further process the Personal Data, unless the Data Controller proves that the Data Management is justified by compelling legitimate reasons, which take precedence over the interests, rights and freedoms of the Data Subject, or which have related to the submission, enforcement or protection of legal claims.

If the Data Management made for direct marketing, then the Data Subject is entitled to protest the processing of its relevant Personal Data for those reasons, including profiling, if it relates to direct marketing.

If the Data Subject protest to the processing of Personal Data for the purposes of direct marketing, then the Personal Data may no longer be processed for this purpose.

The right to protest shall be explicitly brought to the attention of the Data Subject at the latest at the time of first contact, and the relevant information should be displayed clearly and separately from all other information.

By way of derogation from the provisions of Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, the Data Subject may exercise the right to protest by automated means based on technical specifications.

If processing of the Personal Data is made in accordance with subsection (1) of article 89 of the GDPR of the scientific or historical purposes or of statistical purposes, the Data Subject is entitled to protest, for reasons of their own situation, to the processing of the Personal Data related to it, unless the Data Management is necessary for the performance of a task in the public interest.

9. Automated decision making in individual case

The Data Subject has the right not to be covered by a decision based solely on automated Data Management, including profiling, which would have legal effect on it, or would be similarly significant.

The above provision shall not apply if the decision is necessary for the conclusion or performance of the contract between the Data Subject and the Data Controller, or is made possible by EU or Member State laws applicable to the Data Controller, which provide appropriate measures for the protection of the rights and freedoms, and legitimate interests of the Data Subject, or based on the express consent of the Data Subject.

In case of contractual or based on voluntary consent Data Management, the Data Controller shall take appropriate measures to protect the rights, freedoms and legitimate interests of the Data Subject, including at least the right of the Data Subject to request human intervention, to express its views, or to object to the decision.

The above decision shall not be based on the specific categories of Personal Data referred to in subsection (1) of article 9 of the GDPR, unless point a) or b) of subsection (2) of article 9 of the GDPR applies, and appropriate measures have been taken to protect the rights and freedoms, and legal interests of the Data Subject.

10. RESTRICTIONS

EU or Member State laws may restrict the applications of the provisions of articles 12 to 22 of the GDPR and of article 34 of the GDPR, and scopes of rights and obligations set out in article 5 of the GDPR in accordance with the articles 12 to 22 of the GDPR, if the restrictions respect the protection of the fundamental rights and freedoms provided, and it is a necessary and proportional measure taken in accordance with article 23 of the GDPR in a democratic society.

XI. ENFORCING THE RIGHTS OF THE DATA SUBJECT

The Data Controller strives for the Data Subject be able to exercise its rights related to the Data Management in accordance with the laws and all case ends with satisfaction of the Data Subject.

If the protest, complaint, request of the Data Subject related to its Personal Data failed to settle in a reassuring way with the Data Controller, or the Data Subject considers that an infringement has occurred or is imminent, then is entitled to make a report to the Hungarian National Data Protection and Freedom of Information Authority.

Contact details of the Hungarian National Data Protection and Freedom of Information Authority:

Head office: 22/C Szilágyi Erzsébet alley, Budapest, 1125, Hungary
Postal address: P.O. box 5, Budapest, 1530, Hungary
Phone: +36 1 391 1400
Fax: +36 1 391 1410
E-mail: ugyfelszolgalat@naih.hu
Website: https://naih.hu/

In case of illegal Data Management experienced by the Data Subject, the Data Subject may initiate a civil lawsuit against the Data Controller. The lawsuit may also be brought before the court of the place of residence in Hungary of the Data Subject. The Data Subject may find out about the list of regional courts and their contact details on the https://birosag.hu/torvenyszekek/ website.