

**PRIVACY POLICY**  
**INTERNAL ABUSE REPORTING SYSTEM**  
*Last updated on: 24.07.2023.*

**1. The Data Controller**

**The attorney-at-law in charge of whistleblower protection indicated on the website (WP Attorney-at-Law)**

Address: H-1024 Budapest, Ady Endre u. 24.

E-mail: office@panaszdoboz.hu

(hereinafter referred to as: the “Data Controller”).

**2. Data management**

**Your identity will be kept confidential at all stages of the investigation. If you do not provide your personal data, the report may be made, but not investigated.**

Stakeholders and data	Purpose of data management	Retention time	The legal basis of data management	Rights
<b>The reporting party</b>  <i>Personal data provided during reporting: e.g.: name, e-mail address, phone number</i>	Investigation of the complaint, remedying or ending of the conduct that is the subject of the complaint.	Personal data not necessary for the investigation will be deleted immediately.  If no further action has been taken on the basis of the investigation – we will delete the personal data from the investigation documentation after the investigation is completed.	<b>Fulfilling legal obligations</b> The provisions of the Complaints Act <sup>1</sup> regulate the way in which data is handled. <b>If you do not provide your personal data, the report may be made, but not investigated.</b> [Articles 6(1)(c) and 9(2)(g) of the GDPR]	Articles 4.2, 4.3, 4.5

<sup>1</sup> Act XXV of 2023 on Complaints, Notifications of Public Interest and Rules on Reporting Abuses

<p><b>If an investigation is carried out: Person with substantive information on the subject matter of the report</b></p> <p><i>Personal data obtained during the investigation: e.g.: name, e-mail address, phone number</i></p>	<p>Investigation of the complaint, remedying or ending of the conduct that is the subject of the complaint.</p>	<p>Personal data not necessary for the investigation will be deleted immediately.</p> <p>If no further action has been taken on the basis of the investigation – we will delete the personal data from the investigation documentation after the investigation is completed.</p>	<p><b>Fulfilling legal obligations</b> The provisions of the Complaints Act regulate the way in which data is handled. <b>If you do not provide your personal data, it will not be recorded during the investigation.</b> [Articles 6(1)(c) and 9(2)(g) of the GDPR]</p>	<p>Articles 4.2, 4.3, 4.5</p>
<p><b>If an investigation is carried out: Person giving rise to the report</b></p> <p><i>Personal data provided in the report: e.g.: name, position.</i></p> <p><b>Source: The reporting person or the person who has substantial information about the subject matter of the report shall provide the necessary data for identification.</b></p>	<p>Investigation of the complaint, remedying or ending of the conduct that is the subject of the complaint.</p>	<p>Personal data not necessary for the investigation will be deleted immediately.</p> <p>If no further action has been taken on the basis of the investigation – we will delete the personal data from the investigation documentation after the investigation is completed.</p>	<p><b>Fulfilling legal obligations</b> The provisions of the Complaints Act regulate the way in which data is handled. [Articles 6(1)(c) and 9(2)(g) of the GDPR]</p>	<p>Articles 4.2, 4.3, 4.5</p>

<p><b>Recording the voice of a telephone caller</b></p> <p><i>Voice record</i></p>	<p>Investigation of the complaint, remedying or ending of the conduct that is the subject of the complaint.</p>	<p>If no further action has been taken on the basis of the investigation – we will delete the personal data from the investigation documentation after the investigation is completed.</p> <p>If it takes place sooner, until the consent is withdrawn.</p>	<p><b>Consent</b>, which you give by telling the report to the recorder. <b>You may withdraw your consent at any time by contacting us at any of the contact details indicated in Article 1.</b> The withdrawal does not affect the lawfulness of the data management that preceded it. [Articles 6(1)(a) and 9(2)(a) of the GDPR]</p>	<p>Articles 4.1., 4.2., 4.3., 4.4., 4.5., 4.6.</p>
<p><b>Transfer of personal data of the reporting party to the employer with the consent of the reporting party</b></p>	<p>Investigation of the complaint, remedying or ending of the conduct that is the subject of the complaint.</p>	<p>One-off transmission of data</p>	<p><b>Consent</b>, given by e-mail or in writing. <b>You may withdraw your consent at any time by contacting us at any of the contact details indicated in Article 1 until the transmission.</b> The withdrawal does not affect the lawfulness of the data management that preceded it. [Article 6(1)(a) of the GDPR]</p>	<p>Articles 4.1., 4.2., 4.3., 4.4., 4.5., 4.6.</p>

### 3. Recipients:

#### Data processors:

- ✓ The internal abuse reporting website is edited and maintained by **Varga Attila E.V.** (Attila Varga, self-employed sole trader) (contact details: honlap-weboldal.hu/impresszum).
- ✓ The hosting provider is **Magyar Hosting Kft.** (registered office: H-1132 Budapest, Victor Hugo utca 18-22.).
- ✓ To record reports made by a phone call, we use the products of **Rebell Telecommunication Zrt.** (registered office: H-2483 Gárdony, Vörösmarty utca 68.).

- ✓ We use the products of **Microsoft Ireland Operations Limited** (registered office: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521), as our data processor for the processing of the report.

#### **Possible other ways of data transmission:**

- ✓ The personal data may be transferred **to an external body involved in the investigation of the report.**
- ✓ The reporting party's personal data may be disclosed only to **the body that may be competent to investigate the report**, if that body is authorized to process the data by law or if the reporting party has consented to the transmission of the data.
- ✓ If it has become apparent that the reporting party has communicated false data or information in bad faith and there are indications that a criminal offence or irregularity has been committed, his or her personal data **must be transmitted to the body or person authorized to initiate the proceedings**, or, if there are reasonable grounds to believe that he or she has caused unlawful damage or other legal harm to another person, to the body or person authorized to initiate or conduct the proceedings, at the request of the latter.

#### **4. Rights**

In relation to data management, you have the rights detailed in Articles 4.1. to 4.7. If you would like to exercise any of these rights, please write to us using one of the contact details in Article 1.

##### *Identification*

In all cases, we will always need to identify your identity before we can fulfil your request. Unfortunately, if we cannot identify you, we cannot fulfil your request.

##### *Answering the request*

Once identified, we will provide you with information about your request in writing, electronically or, at your request, verbally. Please note that if you have submitted your request electronically, we will respond electronically. Of course, you still have the possibility to request another way.

##### *Administration deadline*

At the latest within 1 (one) month of receiving your request, we will inform you of the action we have taken in response to your request. If necessary, taking into account the complexity of the application and the number of requests, this period may be extended by a further 2 (two) months, of which you will be informed within the 1 (one) month time limit.

We are also obliged to inform you of any failure to take action within the one-month time limit. You can lodge a complaint with the NAIH (Article 5.1) and exercise your right to a judicial remedy (Article 5.2).

##### *Fees for the administration*

The information and action requested is free of charge. The exception is where the request is clearly unfounded or excessive, in particular because of its repetitive nature. In this case, we may charge a fee or refuse the request.

#### **4.1. You can withdraw your consent**

For data management based on your consent, you may withdraw your consent at any time. In such a case, we will promptly delete your personal data relating to that data management. Please note that the withdrawal does not affect the lawfulness of the data management carried out on the basis of the prior consent.

#### **4.2. You can request information (access)**

Where the report concerns a natural person, in exercising his or her right of information and access under the provisions on the protection of personal data, the personal data of the reporting party shall not be disclosed to the person requesting the information.

You can request information on whether your personal data is being managed and if so:

- For what purpose?
- What data is being processed?
- To whom the data are transferred?
- For how long we will keep them?
- What rights and remedies do you have in this regard?
- From whom we received your data?
- Whether we are making automated decisions about you using your personal data? In such cases, you may also request information about the logic (method) we use and the significance and likely consequences of such data processing.
- If you have found that we have transferred your data to an international organisation or a third country (non-EU country), you can ask us to show you how we guarantee the fair processing of your personal data.
- Request a copy of the personal data we process (We may charge a fee based on administrative costs for additional copies.).

#### **4.3. You can ask for a correction**

You may ask us to correct or complete any personal data that has been inaccurately or incompletely recorded about you.

#### **4.4. You can ask for your personal data to be deleted (“forgotten”)**

You can ask us to delete your personal data if:

- The personal data is no longer necessary for the purposes for which it was processed;
- In case of data processing based on your consent;
- If we are found to be unlawfully processing your personal data;
- If your protest is successful;
- If required by EU or national law;
- The data was collected in the context of offering an IT service to children.

We **may not delete** personal data if it is necessary:

- for the purpose of exercising the right to freedom of expression and information;
- to comply with an obligation under Union or Member State law that requires the Data Controller to process personal data or in the public interest;
- for reasons of public interest in the area of public health;
- for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes, in so far as the deletion is likely to render impossible or seriously impair the achievement of the objectives of that data processing; or
- for the establishment, exercise or defence of legal claims.

#### **4.5. You can ask us to restrict the data management**

You may request that we restrict data management if one of the following conditions is met:

- You contest the accuracy of the personal data, in which case the restriction applies for the period of time that allows us to verify the accuracy of the personal data;
- The processing is unlawful, but you oppose the deletion of the data and instead request the restriction of their use;
- We no longer need your personal data for the purposes of data management, but you need it to establish, exercise or defend legal claims;
- You have objected to the data management; in this case, the restriction applies for the period until it is established whether the legitimate grounds of the Data Controller prevail over your legitimate grounds.

In case of restriction, personal data, except for storage, may only be processed with your 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 important public interests of the Union or of a Member State. You will be informed in advance of any lifting of the restriction.

#### **4.6. You can request us to transfer your personal data (right to data portability)**

You have the right to receive your personal data that we manage in a machine-readable format and the right to have that data transferred to another data controller – or at your request – where the processing is based solely on your consent or on a contract with you or on your behalf and takes place in an automated way.

This right does not apply where the data management is necessary for the performance of a task carried out in the public interest. It must not infringe the right to erasure or adversely affect the rights and freedoms of others.

#### **4.7. You can object to the management of your personal data**

You may object to the management of your personal data where the data management is based on a legitimate interest, for direct marketing purposes (e.g. sending a newsletter) or necessary for the performance of a task carried out in the public interest. In this case, the personal data will be deleted, unless the processing is justified by compelling legitimate grounds which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

You also have the right to object to the management of your personal data if the personal data are processed for scientific or historical research purposes or statistical purposes. In this case, the personal data will be deleted unless the data management is necessary for the performance of a task carried out for reasons of public interest.

## **5. Legal remedies**

### **5.1. You can complain to the NAIH**

If you believe that the processing of your personal data is in breach of the provisions of the Data Protection Regulation, you have the right to lodge a complaint with the National Authority for Data Protection and Information Security (NAIH).

NAIH

Chairperson: dr. Attila Péterfalvi

Correspondence address: H-1363 Budapest, P.O.Box: 9.

Address: H-1055 Budapest, Falk Miksa utca 9-11.

Telephone: +36 (1) 391-1400

Fax: +36 (1) 391-1410

Web: <http://naih.hu>

E-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)

### **5.2. Turning to a court**

If you believe that the processing of your personal data is in breach of the provisions of the Data Protection Regulation and that your rights under the Data Protection Regulation have been infringed, you have the right to take legal action.

In Hungary, the tribunal court has jurisdiction to hear the case. According to the preference of the data subject, the lawsuit may also be initiated before the tribunal court according to the place of residence or dwelling place of the data subject. Persons who otherwise do not have any legal capacity in the lawsuit may be a party to the lawsuit, too. The Hungarian National Authority for Data Protection and Information Security (NAIH) can intervene in the case for the sake of success of the data subject. In addition to the provisions of the Data Protection Regulation, the court proceedings shall be governed by the provisions of Act V of 2013 on the Civil Code, Book Two, Part Three, Title XII (§ 2:51 - § 2:54) and other legal provisions applicable to court proceedings.

### **5.3. Compensation and grievance fees**

If the Data Controller causes damage by unlawful processing of the data subject's data or infringes the data subject's right to privacy, the Data Controller may be liable to pay damages. The Data Controller shall be exempt from liability for the damage caused and from the obligation to pay compensation if it proves that the damage or the infringement of the personal rights of the data subject was caused by an unforeseeable cause outside the scope of the data processing.

## **6. Data security**

We will make every effort to implement appropriate technical and organisational measures to ensure a level of data security appropriate to the level of risk, taking into account the current state of science and technology, the cost of implementation, the nature of the data processing and the risk to the rights and freedoms of natural persons.

Personal data will always be treated confidentially, with limited access, encryption and as much resilience as possible, ensuring recoverability in the event of a problem. Our systems are regularly tested to ensure security. In determining the appropriate level of security, we take into account the risks arising from the data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise handled.

We will do our utmost to ensure that persons acting under our control who have access to personal data are only allowed to process that data in accordance with our instructions, unless they are required to do otherwise by EU or Member State law.

## **7. Miscellaneous provisions**

The Data Controller is authorized to amend the provisions included in this Privacy Notice at any time. Any amendment will enter into force at the same time as it is published on the website.