Information on the Processing of Personal Data in connection with Whistleblowing (the "Memorandum")

Introduction

Dear all,

By this memorandum, we inform you as **data subjects** about the principles and procedures for the Processing of your Personal Data and your rights related to the Processing of Personal Data, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation; the "**GDPR**") and Act No. 110/2019 Coll., on Personal Data Processing, as amended (the "**PDPA**").

We respect transparent and fair processing of your Personal Data and its appropriate protection according to the applicable legislation to ensure correct and fair processing. We protect your personal data with the highest security to prevent any unauthorized or accidental access to your personal data, destruction, loss, unauthorized transfers and unauthorized processing. To this end, we take appropriate technical and organisational measures to ensure a level of security appropriate to all potential risks. Persons who come into contact with Personal Data are obliged to maintain the confidentiality of information obtained in connection with the processing of Personal Data.

By means of this Memorandum, we inform you what Personal Data we process about you in connection with your **Report or Concern** made through the **Internal Whistleblowing System** and with the administration of Reports and Concerns and the performance of obligations under the Whistleblower Protection Act.

As personal data protection terms and abbreviations are used in this Memorandum, we have included an explanation of these terms and abbreviations in section **'List of Selected Terms and Abbreviations'** in order to make the content of this Memorandum as clear and comprehensible as possible.

Controller

For the purposes of the GDPR, the company affected by the Report or Concern made via the **Internal Whistleblowing System** is the Controller of your Personal Data (the "**Controller**") that is responsible for compliance with the obligations under applicable personal data protection legislation.

Data subject

The Whistleblower, the persons named by the Whistleblower in the Report, the designated person, the person against whom the Report is directed, the person who raised the Concern and the persons named in the Concern are data subjects, a person identified by the Whistleblower as a witness, a person whose assistance is requested by the designated person in submission the Report, a member of the body.

List of Selected Terms and Abbreviations

TERM/ABBREVIATION	DEFINITION
Personal data	Any information relating to an identified or identifiable natural person; 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
Report	Report under Section 2 of the Whistleblower Protection Act[1]
Whistleblower	an individual who makes a Report
Concern	the provision of information, the submission of an enquiry or a request for consultation relating to any actual or suspected breach of law, EPH Group policies or the internal rules of the Controller which is not a Report
Means of processing	the tools and processes selected for the specific Processing of Personal Data
Legal ground	The condition without which the Processing of Personal Data is **not in any case possible**
Purpose of processing	The objective and purpose of the Controller's activity
OPDP	The **Office for Personal Data Protection** is the supervisory authority under the PDPA. The competences of the central administrative authority related to personal data protection to the extent provided for in the PDPA and other competences laid down in a special law are assigned to the OPDP

[1] *Act No. 171/2023 Coll., on Whistleblower Protection*

Processing	**Any** operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Source of the Personal Data being processed

We obtain your Personal Data **primarily from you**, or from the Whistleblower, or from the person raising a Concern.

Purpose of Processing, Categories of Personal Data being Processed, Legal Ground and Duration of the Processing of Personal Data

We process your Personal Data in relation to the relevant Legal Ground and Purpose of Processing. Non-exhaustive list of processing purposes is given in the following table:

Purpose of processing	Categories of Personal Data	Legal Ground	Duration of Processing[2]
Submission and receipt of Reports and Concerns Assessment of Reports of possible infringements and assessment of Concerns Notification to the Wistleblower of receipt of the Report and of the results of the assessment of the Report Notification to the Whistleblower of receipt of the Concern and of the results of the assessment of the Concern Taking appropriate measures to remedy or prevent the identified situation following the Report or Concern Keeping records of Reports and Concerns	• Identification and contact details (e.g. name, surname, date of birth, contact address of the Whistleblower, data from which the identity of the Whistleblower can be inferred, identification and contact details of the person raising a Concern • Other data (e.g. date of receipt of the Report/Concern, summary of the content of the Report/Concern, details of the person against whom the Report/Concern is directed, date of completion of the assessment of the validity of the Report/Concern, information necessary to investigate the specific case, recordings or transcripts of the investigation, measures to remedy or prevent the infringement)	**Compliance with a legal obligation** **Legitimate Interest** (for Concerns and Reports[3]) Processing is necessary in order to protect the **vital interests**	for a period of 5 years from the date of receipt of the Report or Concern[3] processing period for consent[4]
Audio recording of the Report, the Whistleblower's comment on the transcript of the audio recording		Consent Compliance with a legal obligation	

[2] *In determining the adequacy of the duration of Processing of Personal Data, the following aspects are taken into account (i) limitation periods, (ii) probability of legal claims, (iii) probability and significance of the risks involved, and (iv) any recommendations of supervisory authorities*

[3] *Report from a person who does not perform work or other similar activity for the obliged entity as referred to in Section 2(3)(a), (b), (h) or (i) of the Whistleblower Protection Act*

[4] *If consent is the Legal Ground, then for the period stated in the consent. If the consent is withdrawn, then for a period of 5 years after its withdrawal, in order to prove that the Processing of Personal Data was lawful. Legitimate interest is the legal ground for such Processing.*

Use of the Whistlelink cloud hosting as an Internal Reporting System through which the Whistleblower makes Reports or Concerns; it is also a communication channel with the Whistleblower/the person raising a Concern		Compliance with a legal obligation Legitimate Interest	
Record of advice to the designated person	Personal data contained in the record of advice to the designated person	Compliance with a legal obligation	for a period of 5 years from the date of termination of the activity of the designated person
Proof of the integrity of the designated person	Personal data contained in the criminal record certificate and in the Statement of the designated person, notification of change	Compliance with a legal obligation	for a period of 5 years from the date of termination of the activity of the designated person
Provision of information on the identity of the Whistleblower and the person referred to in Section 4(2)(a) to (h) of the Whistleblower Protection Act	Identity information provided that indicates the relevant consent	Consent	for a period of 5 years from the date of the provision of the identity information
Enforcement of claims of the Controller	• Identification and contact details (e.g. name, surname date of birth, permanent address) • Other data (e.g. data given in the contract documents)	Legitimate Interest	for the time necessary to fulfil the Purpose of the Processing
Control activities in Personal Data protection and data subject requests	Processing of Personal Data in connection with Concerns raised and data subject requests	Compliance with a legal obligation	5 years from the processing of the data subject's request

Method and means of processing

We process your Personal Data by **manual** means (for example, by storing a record of advice) and by **automated** means (by means of ICT, such as a personal computer using Microsoft Office 365 applications, as well as the Controller's or processor's systems via the Whistlelink Internal Reporting System). The Controller **does not use automated decision-making**, **including profiling**, which might affect your rights.

Handling Reports and Concerns

Reports and Concerns made through the Internal Whistleblowing System are processed by the designated person.

Identity information of the Whistleblower and the person named by the Whistleblower in the Report may be disclosed only with written consent unless the designated person is obliged to provide such information to the relevant public authorities under other legislation, e.g. to law enforcement authorities.

Processor

If you make a Report or a Concern through the Whistlelink Internal Reporting System, please note that the Whistlelink service provider and cloud hosting provider, i.e. Whistleblowing Solutions AB https://www.whistlelink.com/data-

security-and-protection/., is also involved in the Processing of Personal Data. The current list of other Whistlelink sub-processors is available at https://www.whistlelink.com/privacy-notice-platform/.

Categories of processors	Activities
IT service provider and software supplier	Provision of IT services, software including service support, administration, development, maintenance of the system and processing of security risk analyses
Service and counselling provider	Provision of services and counselling

Transfer of Personal Data to third countries

The Controller and the processors acting on the Controller's behalf process your personal data primarily in the Czech Republic or in the European Union (EU), where unified data protection is guaranteed in each member state.

Data Subject Rights

- If the Processing of Personal Data is based on your consent, you have the right **to withdraw** your consent **at any time**. In connection with the withdrawal of consent, the Controller informs you that **the withdrawal of consent does not affect the lawfulness of the Processing of Personal Data until its withdrawal**, nor does it affect the Processing of Personal Data on other legal grounds for which your consent is not required.
- You have the right to request **access** to your Personal Data and more detailed information about its Processing.
- You have the right to have your inaccurate or incomplete Personal Data rectified.
- You have the right to **receive** your Personal Data in a commonly used and machine-readable format, allowing it to be transferred to another controller if we have obtained it on the basis of your consent or in connection with the conclusion and performance of a contract and it is processed by automated means.
- You have the right to **object** to the Processing of some or all of your Personal Data.
- You have the right to ask us to **delete** your Personal Data if there is no longer any legal ground for further Processing.
- You have the right to lodge a **complaint** with the OPDP.
- You have the right **not to be subject** to automated individual decision making, including profiling.

Updates to the Memorandum

As the rules and conditions for the Processing and protection of your Personal Data may change, in particular as a result of changes in legislation, or our terms, procedures and methods of Processing and protecting your Personal Data may change, we will inform you of such changes by updating this Memorandum unless such change requires contacting you directly.

Exercise of Data Subject Rights

If you exercise your right pursuant to section **'Data Subject Rights'** by making a request, the Controller **shall always** handle such request of the data subject and shall provide the information without undue delay after receipt of the request, in any case **within one month from receipt of the request. In exceptional circumstances**, this period may be extended by two months, of which the data subject must be informed by the Controller, including the reasons for such extension.

You can send your request to:

- to the address of the Controller's registered office
- to info@epholding.cz
- to the e-mail address of the chief protection officer cpo@epholding.cz
- alternatively, you can contact the Controller using the following telephone number: **+420 232 005 200.**

To make it easier to exercise your rights, you can use the sample **Data Subject Request** form available here.

If you have reasonable suspicion that there has been a breach of law in connection with Personal Data protection, **you have the right to lodge a complaint with the Office for Personal Data Protection, Pplk. Sochora 727/27, 170 00 Prague 7 – Holešovice, email:** stiznosti@uoou.cz, use the form available on the website of the Office for Personal Data Protection https://uoou.gov.cz/verejnost/stiznost-na-spravce-nebo-zpracovatele.