Information on Data Processing to Employees and Board Members (the "Memorandum")

Introduction

Dear employees, board members,

This Memorandum is to inform you as **data subjects** on the principles and procedures applicable to the processing of your personal data and on your rights related to the processing of this 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/ES (General Data Protection Regulation; hereinafter the "**GDPR**") and in accordance with Act No. 110/2019 Coll., on Processing of Personal Data, as amended (hereinafter the "**PDPA**").

Our company respects 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, destruction, loss, unauthorized transmissions, or unauthorized processing of your personal data. For this purpose, we comply with the relevant technical and organisational measures to ensure an appropriate level of security with respect to all possible risks. Persons who handle personal data are obliged to maintain confidentiality of the information obtained in connection with the processing of this data.

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.

In addition to the information contained in this Memorandum, further details on the processing of your personal data will be available in the relevant internal rules of the Controller.

Controller

The Controller of your personal data is the company **HX Medical a.s.**, company reg. No. 24092495, having its registered office at náměstí Marie Schmolkové 3493/1, Strašnice, 100 00 Praha 10, entered in the Commercial Register under file No. B 30274 /MSPH, with which you have concluded your employment contract (or a similar contract) or your executive service agreement (hereinafter the "**Controller**") who is responsible for discharging the obligations under the applicable data protection laws.

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.
Special categories of personal data	Personal data revealing racial or ethnic origin, political opinions, religion or philosophical beliefs or trade union membership, and processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning health or data concerning a natural person's sex life or sexual orientation.
Data subject	The natural person to which the personal data relates. A data subject is deemed to be identified or identifiable if, based on one or several personal data, the data subject's identity can be directly or indirectly determined.
Controller	The natural or legal person, public authority, agency or another body, which, alone or jointly with others, determines the purposes and means of processing of personal data.
Processing	**Any** operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Purpose of processing	The objection and purpose of the Controller's activity
Means of processing	The tools and processes selected for specific processing of personal data.
Legal ground	The condition without which the processing of personal data is **not in any case possible**.
Processor	A natural or legal person, public authority, agency or another body which processes personal data on behalf of the Controller.
Recipient	A natural or legal person, public authority, agency or another body to which the personal data is disclosed, whether a third party or not. The Recipient has the legal, contractual or other authority to process personal data. These are other controllers or processors, such as tax, administrative or regulatory authorities. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with the Member State law shall not be regarded as recipients; the processing of that personal data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
Third party	A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.
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.

Processed personal data

The Controller and the processor that processes personal data on behalf of the Controller, process, with regard to the relevant legal ground and purpose of processing, in particular the following categories of personal data:

- **identification, authentication and address data**: name, surname, academic degree(s), date of birth, ID card data, permanent address, temporary address, address for service or other contact address, nationality, place and state or birth, birth number, handwritten signature and digital signature
- **contact details**: telephone number, email address, data box ID
- **electronic details**: IP address, authentication certificates, digital signature certificates
- **personal data related to the employment (or any similar) contract**: bank account number, payroll details, education, criminal matters, identification data of children and family members, knowledge of foreign languages, personal number
- **in specific cases special categories of personal data**

An overview of the personal data processed by the Controller is available in the relevant internal rules of the Controller.

Source of the personal data being processed

The Controller obtains your personal data **primarily from you** when negotiating an employment contract or service contract and in connection with their performance, or from third parties that mediate such negotiations. Also, the Controller obtains your personal data **from publicly available sources** (such as the Commercial and Trade Registers) or **from public authorities**.

Video surveillance system

The Controller hereby informs you that the company **Health Uncompromised a.s.,** company reg. No. 23163551, having its registered office at náměstí Marie Schmolkové 3493/1, Strašnice, 100 00 Praha 10, entered in the Commercial Register under file No. B 29634 /MSPH, operates a camera surveillance system with recording for the purpose of protecting property, life, and the health of persons present in the monitored area (at the address Náměstí Marie Schmolkové 3493/1, Strašnice, Prague. The use of camera surveillance systems is indicated by information signs placed on the relevant premises. Information on the processing of personal data through camera surveillance systems can be found on the website https://hx.clinic/.

The Controller further informs you that at designated workplaces, the company **EP Investment Advisors, s.r.o.**, Company ID No. **26687259**, with its registered office at **Pařížská 130/26, Prague 1 – Josefov, ZIP code 110 00**, registered in the Commercial Register under file No. **C 87354/MSPH**, operates a camera surveillance system with recording for the purpose of protecting property, life, and the health of persons present in the monitored area. The use of camera surveillance systems is indicated by information signs placed on the relevant premises. Information on the processing of personal data through camera surveillance systems can be found on the website www.epholding.cz.

Purpose and duration of the processing of personal data

The Controller processes your personal data in particular for the purposes listed below, based on the respective legal ground.

The **period for which the Controller is entitled to process your personal data** depends on the purpose of processing (for example, payroll sheets or accounting records containing data required for pension insurance purposes are archived by the Controller for 30 years, payroll sheets or accounting records containing data required for pension insurance purposes kept on an old-age pensioner are archived for 10 years).

Non-exhaustive list of processing purposes:

- processing of personal data of employees in connection with personnel matters
- processing of personal data of employees in connection with payroll matters
- processing of personal data in connection with arranging occupational medical examinations
- processing of personal data of board members for the purpose of registration in public registers
- processing of personal data in the context of archiving documents
- processing of personal data in the context of enforcing the Controller's claims

An overview of the purposes of processing and the processing periods is available in the relevant internal rules of the Controller.

Legal ground for the processing of personal data

Article 6 GDPR distinguishes **six types** of legal grounds for the processing of personal data; **four legal grounds** that are **most relevant** to the Controller are **shown below.** The Controller processes your personal data as follows:

- processing is necessary for the **performance of a contract**
- processing is necessary for **compliance with a legal obligation** to which the Controller is subject (e.g., when preparing data for the calculation of statutory health and social insurance contributions)
- processing is necessary for the purposes of **the legitimate interests pursued by the Controller or by a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child
- on the basis of your **consent**, only if no other legal ground for data processing (such as consent to use a photograph) can be applied

It is not possible to conclude a contract without providing the personal data necessary for the performance of the contract and the fulfilment of legal obligations. You have right to object to the processing of personal data for the purposes of legitimate interests. You have the right to withdraw your consent at any time. Please be informed that the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

An overview of the legislation related to the processing of personal data for compliance with a legal obligation is available in the relevant internal rules of the Controller.

Manner and means of processing

The Controller and the processor processing personal data on behalf of the Controller process your personal data by **manual** means (such as by placing the employment contract in paper form in the employee's personnel file) 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).

In processing your personal data by automated means, the Controller **does not apply automated decision-making, including profiling,** that might affect your rights.

In accordance with applicable law, the controller informs you that it uses artificial intelligence tools ("AI systems") embedded in Microsoft cloud services. Further information can be found here: Frequently asked questions: AI, Microsoft Copilot, and Microsoft Designer. These IA systems include tools for identifying security incidents and spam filtering, which use AI to identify and separate unsolicited emails from legitimate communications. They also contribute to protecting user identities, managing Office 365 cloud applications, and safeguarding end-user devices.

Another tool used is Microsoft Copilot, an AI-powered digital assistant designed to help users with various tasks and activities in the Office 365 environment. Copilot uses OpenAI's ChatGPT technology, a form of generative AI that mimics human conversation by understanding user queries and responding to them in natural language. Please keep in mind that you are interacting with an AI and not a live human.

AI-generated content and output may contain inaccuracies, biases or sensitive material because the AI is trained on data from the internet and other digital sources. Additionally, the AI may not be aware of recent events, which could lead to potential inaccuracies. Please avoid disclosing sensitive and private company data when interacting with a generative chatbot tool.

Microsoft's AI services are built on a comprehensive approach to security, compliance and privacy. For more information on privacy, see Data, Privacy, and Security for Microsoft 365 Copilot below.

Processor

The Controller processes your personal data through its employees who need access to the personal data in order to perform their duties and who are obliged to maintain confidentiality of all facts and information of which they become aware in the course of their employment.

In addition, the **processor's** employees have access to your personal data, only to the extent necessary to carry out their work for the Controller. We enter into a written **Data Processing Agreement** with all our processors, establishing appropriate safeguards for the security of your personal data. These include, for example, companies providing payroll processing for the Controller or providers of IT services and software providers providing programming or other technical support services.

An overview of the processors processing personal data on the Controller's behalf is available in the relevant internal rules of the Controller.

Recipients of personal data

The Controller may, in certain circumstances, transfer your personal data to recipients (other controller, processor) and third parties.

These **recipients** include, for example, public authorities to whom personal data of employees are routinely transferred for the purpose of keeping tax records or calculating social security or health insurance contributions:

- Czech Social Security Administration
- health insurance companies
- tax authorities and bailiff offices in connection with the employer's normal reporting and tax obligations

However, where public authorities require personal data in the framework of a particular inquiry, they are not considered to be recipients but **third parties**.

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. Quite exceptionally, your personal data may be processed outside the EU, for example, in a computer system whose servers are located outside the EU. In that case, we would select a contractual partner that will meet the conditions for secure data transfer in accordance with the applicable legislation. We will inform you in an appropriate manner about the specific measures and procedures, about to whom and to which countries your

personal data is disclosed/transferred, under which conditions, how your data is protected, and about the risks involved.

Rights of data subjects

- 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 the processing of data for other legal reasons 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 other legal ground for the 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.

This Memorandum was last updated on 3. 9. 2026.

Data Protection Officer

HX Medical a.s. has appointed a Data Protection Officer. Contact details for the Data Protection Officer: milena.segecova@epholding.cz.

Exercise of data subject rights

Where you submit **a request** to exercise your rights as listed in the section entitled **'Data Subject Rights'** of this memorandum, the controller is **always obliged** to deal with such a request from the data subject and must provide the information without undue delay upon receipt of the request, and in any event **within one month of receiving the request. In exceptional cases,** this period **may** be extended by two months, in which case the data controller must inform the data subject of this, including the reasons for such an extension.

You may send your request:
a. in writing to the address náměstí Marie Schmolkové 3493/1, Strašnice, 100 00 Prague 10
b. to the Data Protection Officer, whose contact details are: HX Medical a.s., Data Protection Officer, náměstí Marie Schmolkové 3493/1, Strašnice, 100 00 Prague 10 or
by email to milena.segecova@epholding.cz

To make it easier to exercise your rights, you may use the template form marked **'Data Subject Request**'.

If you have reasonable grounds to suspect that there has been a breach of the law in relation to the protection of personal data**, 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 ; for this purpose, you may use the form available on the Office for Personal Data Protection's website https://uoou.gov.cz/verejnost/stiznost-na-spravce-nebo-zpracovatele.