Information on the processing of personal data for clients (hereinafter referred to as the "memorandum")

Introduction

Dear clients,

by means of this memorandum, we would like to inform you, as data subjects, of the principles and procedures governing the processing of your personal data and of your rights in relation to the processing of such data, in accordance with Regulation (EU) 2016/679 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; hereinafter referred to as the "GDPR") and Act No. 110/2019 Coll., on the processing of personal data, as amended (hereinafter referred to as the "ZZOÚ").

Our company respects the transparent and fair processing of your personal data and ensures its proper protection in accordance with applicable legislation to guarantee fair and ensure processing. We protect your personal data with the highest level of security to prevent any unauthorised or accidental access to your personal data, destruction, loss, unauthorised transfers or unauthorised processing. To this end, we implement appropriate technical and organisational measures to ensure a level of security commensurate with all possible risks. Persons who come into contact with personal data are obliged to maintain confidentiality regarding information obtained in connection with the processing of such data.

Given that this memorandum refers to terms relating to data protection and also uses abbreviations, we have included an explanation of the terms and abbreviations used in the section entitled 'List of selected terms and abbreviations' in this memorandum, in order to present the content of this text to you in an even clearer form.

The role of HX Medical a.s.

The specific nature of the services provided gives rise to a situation in which **HX Medical a.s.**, Company ID No.: 24092495, with its registered office at náměstí Marie Schmolkové 3493/1, Strašnice, 100 00 Prague 10, registered in the Commercial Register maintained by the Municipal Court in Prague under file no. B 30274 (hereinafter referred to as "HX Medical" or "the controller"), acts in two distinct roles, which are essential for understanding your rights.

As **an independent controller**, HX Medical processes your personal data for the purposes of providing healthcare services and fulfilling the associated legal obligations, in particular the maintenance of medical records in accordance with Act No. 372/2011 Coll., on healthcare services and the conditions for their provision, as amended (hereinafter referred to as the "Healthcare Services Act"). In this capacity, HX Medical independently determines the purposes and means of processing and bears full responsibility for them. HX Medical is an authorised provider of healthcare services; all healthcare, diagnostics, treatment and the issuing of medical reports are carried out exclusively by HX Medical's medical staff.

HX Medical acts as **a joint controller** together with **Health Uncompromised a.s.**, Company ID No.: 23163551, with its registered office at náměstí Marie Schmolkové 3493/1, Strašnice, 100 00 Prague 10, registered in the Commercial Register maintained by the Municipal Court in Prague under file no. B 29634 (hereinafter "Health Uncompromised"), in areas where both companies jointly and in a coordinated manner determine the purposes and means of processing your health data via the HUX platform. HX Medical's healthcare staff works with the HUX platform to coordinate your preventive care.

Health Uncompromised a.s. also acts as a processor for HX Medical in the operation, administration, technical support, maintenance and development of the HUX software system — a proprietary application for the HX Medical clinic. In this capacity, Health Uncompromised processes personal data exclusively on the instructions of

HX Medical and solely for the purpose of ensuring the technical availability, integrity, security and functionality of the HUX system.

List of selected terms and abbreviations

TERM AND ABBREVIATION	MEANING
Personal data	Any information relating to an identified or identifiable natural person; an identifiable natural person is a natural person 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 data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning a natural person's health or sex life or sexual orientation.
Data subject	A natural person to whom the personal data relates. A data subject is considered to be identified or identifiable if their identity can be ascertained, directly or indirectly, on the basis of one or more items of personal data.
Controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the 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 any other form of disclosure, alignment or combination, restriction, erasure or destruction.
Purpose of processing	The purpose of the controller's activities and their rationale
Means of processing	Tools and procedures selected for the specific processing of personal data.
Legal basis	A legal basis, or legal ground, is a condition without which the processing of personal data is not possible under any circumstances.
Processor	A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.
Recipient	A natural or legal person, public authority, agency or other body to whom personal data are disclosed, whether a third party or not. The recipient has a legal, contractual or other authority to process personal data. These include other controllers or processors, such as tax, administrative or regulatory authorities. However, public authorities which may receive personal data in the course of a specific inquiry in accordance with Member State law are not considered recipients; the processing of such personal data by these public authorities must comply with the applicable data protection rules for the purposes of the processing.
Third party	A natural or legal person, public authority, agency or other body other than the data subject, the controller, the processor or a person directly under the authority of the controller or processor, which is authorised to process personal data.
ÚOOÚ	The supervisory authority under the Personal Data Protection Act is the Office for Personal Data Protection. It is entrusted with the powers of a central administrative authority in the field of personal data protection to the extent specified by the Personal Data Protection Act and other powers specified by a special legal regulation.

Subject matter of the contract and nature of the services provided

On the basis of the contract concluded with you, HX Medical, as an authorised healthcare provider, provides you with healthcare within the agreed scope. The contractual relationship also includes access to the HUX application's client environment, through which health data is shared, preventive care is coordinated, and communication with HX Medical's healthcare staff takes place.

HX Medical is a healthcare provider within the meaning of the Healthcare Services Act. All healthcare, diagnostics, treatment and the issuing of medical reports are carried out exclusively by HX Medical's medical staff. The HUX platform is operated by Health Uncompromised as a technology partner of HX Medical and serves exclusively as a tool for clinical data management, care coordination and communication with the client — not as an independent healthcare provider.

Source of personal data processed

We obtain your personal data directly from you — when concluding a healthcare contract, during the provision of healthcare services, via the HUX client environment, when communicating with our company, or when using the services provided. Some of your personal data, in particular medical records and clinical data, is generated by HX Medical's healthcare staff as part of the provision of healthcare and recorded in the HUX system. Further data may be transferred from wearables integrated into the HUX app, provided you have given your consent or where their processing is otherwise justified by a legal basis.

CCTV system

The Data Controller hereby informs you that at the address Náměstí Marie Schmolkové 3493/1, Strašnice, Prague, the company **Health Uncompromised** operates a CCTV system with recording, for the purpose of protecting property, life and the health of persons moving within the monitored area, and also for the purpose of obtaining evidence for the Czech Police and resolving insurance claims. These are static cameras capturing images. Information signs indicate the use of CCTV systems. Recordings from the CCTV system are retained for a period of 30 days, after which they are automatically deleted. Further information can be found on the website https://hx.clinic/zpracovani-osobnich-udaju/.

The Data Controller further informs you that at designated premises, **EP Investment Advisors, s.r.o.**, Company ID No. 26687259, with its registered office at Pařížská 130/26, Prague 1 – Josefov, postcode 110 00, registered in the Commercial Register under file no. C 87354/MSPH, data box 89pegns, a CCTV system with recording, for the purpose of protecting property, life and health of persons moving within the monitored area. Information signs located on the relevant premises inform visitors of the use of CCTV systems. Guidance on the processing of personal data via CCTV systems can be found on the website www.epholding.cz.

Purpose and legal basis for the processing of personal data

We process your personal data for the purposes set out below, and for each purpose we also state its legal basis within the meaning of Articles 6 and 9 of the GDPR; in particular, these are:

Purpose of processing	Legal basis
Provision of healthcare services and maintenance of medical records	Article 6(1)(c) of the GDPR, Article 9(2)(h) of the GDPR
Performance of the healthcare contract	Article 6(1)(b) of the GDPR, Article 9(2)(h) of the GDPR
Operation and administration of the HUX application — provision of access to the client environment	Article 6(1)(b) of the GDPR
Coordination of preventive care via HUX (joint controller with Health Uncompromised)	Article 6(1)(b) GDPR, Article 9(2)(h) GDPR
Compliance with legal obligations (record-keeping, archiving, reporting)	Article 6(1)(c) of the GDPR

Purpose of processing	Legal basis
Protection of the controller's legitimate interests (debt recovery, protection of rights)	Article 6(1)(f) of the GDPR
Sending commercial communications and marketing messages	Article 6(1)(a) of the GDPR

The processing of your health data, as a special category of personal data within the meaning of Article 9 of the GDPR, is necessary for the provision of healthcare, the maintenance of medical records and the coordination of preventive care via the HUX platform. The legal basis for this processing is Article 9(2)(h) of the GDPR. To the extent that the processing of health data is subject to your consent, the legal basis is Article 9(2)(a) of the GDPR.

Categories of personal data processed

Depending on the nature of the services you use, we process the following categories of personal data:

Identification and contact details: first name and surname, date of birth, personal identification number (where necessary for maintaining medical records), residential address, email address, telephone number, and, where applicable, identity card number or insurance number.

Contractual and payment data: data necessary for the conclusion and performance of a healthcare contract, billing details, information on payments made.

Health and clinical data (special categories pursuant to Article 9 of the GDPR): medical history, results of examinations and diagnostic tests, medical records maintained in the HUX system and other HX Medical systems, treatment plans and medical protocols set up in the HUX system, records of the course of healthcare provided, data from wearables integrated into the HUX application.

Communication data: the content of your communication with HX Medical healthcare staff via the HUX client environment, records of email and other electronic communications.

Technical and operational data: login details for the HUX application, access logs, technical device identifiers, IP address.

Joint controllership

In areas where HX Medical and Health Uncompromised jointly and in a coordinated manner determine the purposes and means of processing your personal data, they act as **joint controllers** within the meaning of Article 26 of the GDPR. Joint controllership applies in particular to the following areas:

Area	Description
Care coordination	Sharing of client clinical data between HX Medical healthcare staff and the HUX platform operated by Health Uncompromised a.s. for the purpose of coordinating preventive care
Data sharing via HUX	Making the client's health data available in the HUX application interface to both contracting parties simultaneously
Setting treatment protocols	Jointly determining the structure and content of treatment plans within the HUX system
Communication with the client via HUX	Processing of communication with the client via the HUX client portal, where the content of the communication is determined by both parties

An agreement has been concluded between the two joint controllers in accordance with Article 26 of the GDPR. Pursuant to the joint arrangement under Article 26 of the GDPR, HX Medical a.s. is the primary point of contact for exercising your rights in relation to jointly processed data. However, you may exercise your rights against each of

the companies separately; each controller is obliged to process your request. The key elements of the agreement are available on request from the Data Protection Officer.

Recipients and processors of personal data

Within HX Medical, access to your personal data is restricted to employees and healthcare staff whose job roles require it, and only to the extent strictly necessary for the performance of their duties and the fulfilment of their obligations towards you as a patient or client. HX Medical uses processors to ensure the technical infrastructure, system operability and other support activities. Written data processing agreements containing safeguards for the security of your personal data have been concluded with all processors.

Recipient/Processor, in particular:	Identification
MasterDC s.r.o.	Company ID: 26277557, Purkyňova 3030/35e, Brno
Health Uncompromised a.s.	Company ID: 23163551, náměstí Marie Schmolkové 3493/1, Strašnice, 100 00 Prague 10
MAGICWARE s.r.o.	Company ID: 62576836, Krohova 2212/75, Prague 6
Microsoft Ireland Operations Ltd. (Azure)	IE 4390051E, One Microsoft Place, Dublin
EP Investment Advisors, s.r.o.	Company ID: 26687259, Prague 1- Josefov, Pařížská 130/26, Postcode 11000
STAPRO s.r.o. (FonsGalen)	Company ID: 13583531, Pernštýnské náměstí 51, 530 02 Pardubice
Attio	42 St John's Square, 2nd Floor, London EC1M 4EA, United Kingdom
Digital factory s.r.o. (Signi)	Company ID: 06988377, Sokolovská 694/102a, 186 000 Prague 8
Medevio s.r.o.	Company ID: 09675400, Thámova 289/13, Karlín, 186 00 Prague 8
REPROMEDA s.r.o.	Company ID: 255 57 246, Studentská 812/6, 625 00 Brno
CITYLAB s.r.o.	Company ID: 28442156, Seydlerova 2451/8, Postcode 158 00 Prague
SPADIA LAB a.s.	Company ID: 28574907, Máchova 619/30, 741 01 Nový Jičín

Transfer of personal data to third countries

Your personal data is processed primarily within the Czech Republic or, where applicable, within the European Union. In very exceptional cases, your personal data may be processed outside the EU, particularly in a system whose servers are located outside the EU. In such a case, we would select a contractual partner that meets the conditions for secure data transfer in accordance with applicable legislation. To provide the technical infrastructure, HX Medical a.s. uses Attio, to which communication and operational data (in particular clients' contact details and communication records) may be transferred. The transfer of personal data to the United Kingdom is carried out on the basis of the European Commission's adequacy decision. If you have any questions regarding the transfer of data abroad, please contact the Data Protection Officer.

Method of processing personal data

We process your personal data both manually and automatically. Automated processing takes the form of operations in a cloud environment, including in particular storage, reading, structuring, searching, backing up, encryption and monitoring of access within the HUX system and the FonsGalen outpatient information system. Personal data is not subject to automated decision-making or profiling.

Duration of personal data processing

We retain your personal data for the period strictly necessary to fulfil the purpose for which it is processed, and for the period specified by the relevant legislation.

Categories of data	Retention period
Contractual documentation and data necessary for the performance of the contract	For the duration of the contractual relationship and for a further period of 10 years following its termination (limitation periods under the Civil Code)
Medical records and documentation	For the period specified by Act No. 372/2011 Coll., on healthcare services, and the relevant implementing regulations (generally 10 years, longer for selected categories)
Accounting and tax documents	For a period of 10 years in accordance with Act No. 563/1991 Coll., on Accounting
Communication with the client	For the duration of the contractual relationship and for 5 years after its termination
Marketing communications (subject to consent)	Until consent is withdrawn, for a maximum of 3 years from the date of consent
Technical and operational logs	Usually 12 months

Rights of the data subject

As a data subject, you have the following rights in relation to the processing of your personal data, which you may exercise by contacting the controller using the contact details provided above.

- Right of access: you have the right to obtain confirmation from the controller as to whether or not your personal data is being processed, and if so, you have the right to access such personal data and information regarding the purposes of processing, the categories of personal data concerned, the recipients, the retention period and other matters set out in Article 15 of the GDPR. The controller will provide you with a copy of the personal data being processed.
- Right to rectification – you have the right to have inaccurate personal data concerning you rectified and, taking into account the purposes of the processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
- Right to erasure — "right to be forgotten" — you have the right to have your personal data erased if any of the grounds set out in Article 17(1) of the GDPR apply — in particular where the personal data are no longer necessary for the purposes for which they were collected, or where you withdraw your consent and there is no other legal basis for processing. This right does not apply if processing is necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims, or if other exceptions under Article 17(3) of the GDPR apply. In relation to health data held as part of medical records, this right is limited by the obligations arising from the Health Services Act.
- Right to restriction of processing – you have the right to restriction of processing if you contest the accuracy of the personal data (for the duration of the verification of accuracy), the processing is unlawful and you oppose erasure, the controller no longer needs the data but you require it for the establishment, exercise or defence of legal claims, or you have objected to the processing (for the duration of the verification of whether the controller's legitimate grounds override your interests).
- Right to data portability – you have the right to receive the personal data you have provided to the controller and which is processed automatically on the basis of a contract or consent, in a structured, commonly used and machine-readable format, and the right to transmit this data to another controller without the controller preventing this. At your request, where technically feasible, the data may be transferred directly to another controller.
- Right to object – you have the right to object at any time to the processing of your personal data carried out on the basis of the controller's legitimate interests (Article 6(1)(f) of the GDPR). The controller shall no longer process your personal data unless it demonstrates compelling legitimate grounds for the processing which override your interests, rights and freedoms, or for the establishment, exercise or defence of legal claims. If you object to processing for direct marketing purposes, the controller shall cease processing personal data for such purposes without further ado.
- Right to withdraw consent – where 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 prior to the withdrawal, nor does it affect the processing of data on other legal grounds for which your consent is not required.

- **Right not to be subject to automated decision-making –** you have the right not to be subject to any decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you, unless permitted by Article 22(2) of the GDPR.
- **Right to lodge a complaint with a supervisory authority –** you have the right to lodge a complaint with the relevant supervisory authority if you believe that the processing of your personal data infringes the GDPR or other data protection legislation.

Possible updates to this memorandum

Given that the rules and conditions governing the processing and protection of your personal data may change, particularly as a result of changes in legislation, or that our terms, procedures and methods for processing and protecting your personal data may change, we will inform you of such changes by updating this memorandum, unless such a change requires us to contact you directly.

This memorandum was last updated on 3 September 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.