

Addendum on Commissioned Data Processing in accordance with GDPR Art. 28

between

(1) **Healthentia SaaS BENEFICIARY** (hereinafter, the “**Company/Data Controller**”)

and

(1) **INNOVATION SPRINT SRL (iSPRINT)** incorporated in Belgium, whose registered office is at **Clos Chapelle-aux-Champs 30, 1200 BRUSSELS** (hereinafter the **Contractor/Data Processor**)

each a “party” and together the “parties”,

HAVING NOTED THAT

- (A) (EU) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data (hereinafter “GDPR”) guarantees that personal data processing is conducted with due respect for fundamental rights and freedoms as well as dignity of the person concerned, with particular reference to the right to protection of personal data;
- (B) An agreement or purchase order was concluded between the parties related to the use of Healthentia SaaS solution, hereinafter referred to as the **Agreement**.
- (C) In the context of compliance with the legal provisions for the protection of personal data, data processing by the Data Controller is conducted for serving legitimate processing purposes as defined by the requirements set in GDPR and in accordance with the applicable legal and regulatory framework for processing personal data.
- (D) Data Controller guarantees that the data subjects have been duly informed and have agreed to make their information available to the Data Processor.
- (E) This Addendum, which regulates the commissioned processing of personal data, is considered as an Annex to the Agreement. The Company is and remains the Controller, as defined by data protection legislation, for the personal data processed by the Contractor in accordance with this Addendum and the instructions issued by the Company.
- (F) In light of this processing, the parties have agreed to enter into this Addendum to address the compliance obligations imposed pursuant to the Regulation (EU) 2016/679;

AGREE THAT

INNOVATION SPRINT SRL is **EXTERNAL PROCESSOR FOR THE PROCESSING OF PERSONAL DATA**, pursuant to and for the purposes of the provisions contained in Art. 4.8 and 28 of GDPR, regarding the processing of personal data recorded in Healthentia on behalf of the Data Controller.

These activities will be executed based on requirements of the Company in the context of the Agreement.

iSPRINT, as “*Processor for the processing of personal data*”, must comply with operational provisions as set out below.

- Data processing shall be carried out in full compliance with current legislative predictions regarding the protection of personal data and taking account of the measures and official statements issued by the Belgian Data Protection Authorities for the Protection of Personal Data.
- The Processor, in its capacity of "Processor of data processing", is authorised to proceed with the organization of any operation of data processing within the limits established both by the Agreement and by the applicable provisions of GDPR. To this end, "processing" is defined, in accordance with Art. 4 of GDPR, as *"any operation or series of operations, even performed without the aid of electronic means upon personal data or personal data sets such as collection, recording, organization, structuring, storing, adaptation or alteration, extraction, consultation, use, disclosure by transmission, dissemination or otherwise making available, comparing or interlinking, limiting, deletion or destruction"*.
- The Processor, in order to ensure compliance with the principle of "Data protection by design and by default" under Art. 25 of GDPR shall undertake to determine the means of data processing and to implement appropriate technical and organizational measures according to Art. 32 of GDPR before the start of the activities.
- The Processor shall perform those data processing operations functional to the tasks assigned to it, provided, however, that these are not incompatible with the purposes for which the data were collected. Should the need arise to carry out processing operations on different and exceptional personal data than those normally run, the Processor shall notify the Controller of data processing.
- The Processor shall activate the required business processes, in order to identify and educate the persons entitled to the processing of personal data, organizing their tasks so that individual processing operations be consistent with the provisions of this Addendum, and that, on the basis of given instructions, processing operations do not deviate from the purposes for which the data were collected and processed. Moreover, the Processor shall ensure that the persons authorized to data processing be bound by a legal obligation of confidentiality.
- The Processor shall undertake to guarantee the adoption of the security measures referred to in Article 32 of GDPR. In particular, given the state of the art of the security measures adopted for data protection, and the nature, object, context and purposes of the processing, as well as on the basis of results derived from analysis of the risks of varying probability and severity to the rights and freedoms of individuals which result in particular from destruction, loss, alteration, unauthorized disclosure of or access, whether accidental or unlawful, to personal data transmitted, stored or otherwise processed, the Processor shall implement the appropriate organizational actions for optimizing such measures and ensure a level of security appropriate to the risk. These include, among others:
 - a) The encryption of personal data;
 - b) Suitable measures to guarantee the confidentiality, integrity, availability and resilience of processing systems and services;
 - c) Appropriate measures to ensure the ability to restore in a timely manner the availability of and the access to personal data in the event of physical or technical accident;
 - d) Procedures to regularly test, verify and assess the effectiveness of the technical and organizational measures in order to guarantee the security of data processing.
- The Processor, after completion of data processing services, shall take all necessary measures in order to delete all copies and return all personal data in any format and/or media, upon instructions given by the Controller.
- The Processor shall assist the Controller in ensuring compliance with the obligations laid down in Articles 32 to 36 of GDPR, considering the nature of data processing and information available to the Contractor itself as Data Processor. Moreover, the Processor shall assist the Data Controller by

means of appropriate technical and organizational measures when it is necessary to give effect to specific requests regarding the exercise of the rights of the party concerned under Art. 12 of GDPR.

- In accordance with Art. 33 paragraph 2, the Processor, should it become aware of a breach of personal data, must promptly and without undue delay inform the Controller.
- Moreover, the Processor undertakes to:
 - Identify, within its organization, the subjects to whom the roles of System Administrators, Database Administrators and/or Network Administrators shall be assigned and give instructions to these subjects and monitor their activities;
 - Assign to the above mentioned subjects a user id that contains references that can be easily connected to the identity of the Administrators and that guarantees compliance with the following rules:
 - Prohibition to assign generic user IDs and already assigned, also at different times;
 - Deactivation of user IDs assigned to Administrators who no longer need to access data.
 - Associate the user ID assigned to the Administrators with a password that has the following features:
 - Minimum length of 8 characters;
 - Change at first connection and sub sequentially at least every 90 days.
- Ensure that access profiles, in particular for users with administrative privileges, comply with the principle of need-to-know, i.e., that no higher rights are assigned than those strictly necessary to perform ordinary work activities. User positions with administrative privileges must be used only to perform the assigned tasks.
- Within the limitations of the task assigned, make available, when formally requested, the following information regarding the Administrators: successful logins, failed logins, logouts.

Pursuant to art. 28 paragraph 2 of the GDPR, the Controller authorizes the Processor to engage third parties for the implementation of specific activities which fall within the scope of the Addendum.

The Processor shall inform the Controller promptly and shall appoint the Processors imposing, by way for an agreement, the same obligations with respect to the protection of personal data included in this Addendum, specifically proving sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR.

At the time of signature of this Addendum, the Controller agrees that the Processor may exploit the services offered by the following sub-processors:

Microsoft Ireland Operations Limited.
One Microsoft Place, South County Business Park, Leopardstown,
Dublin 18 D18 P521

and:

Enghouse Interactive (UK) Ltd
Imperium, Imperial Way
Reading, Berkshire
RG2 0TD
United Kingdom

By signing this Addendum, the Processor accepts its role and, as provided by Art. 28 of GDPR, hereby declares that all services covered by the **Agreement** shall be executed in compliance with the

provisions contained in GDPR and in respect of the instructions given by the Data Controller, who can require periodic checks on compliance with the provisions therein.

The validity of this document shall also be extended to any further contract extensions; any other agreement remains fully in force and unaffected.

IN WITNESS WHEREOF, AND IN THE ACKNOWLEDGEMENT THAT THE PARTIES HAVE DULY SIGNED BELOW AND BY DOING SO HAVE ACCEPTED AND APPROVED EACH AND EVERY PROVISION OF THIS ADDENDUM.

The Data Controller

The Data Processor
Innovation Sprint Srl