HEALTH DATA HOSTING ADDENDUM

Foreword

The parties have entered into the Genesys Cloud Terms and Conditions (the "**Agreement**") and a Data Processing Agreement (the "**DPA"**) and hereby agree to change the contractual clauses with the following HDS (Hébergeur de Données de Santé) Addendum (the "**Addendum**"). The Addendum outlines the specific responsibilities and standards for the secure processing and hosting of health data in compliance with French law and HDS certification requirements and is only applicable to Hosting Services containing Health Data, both as defined below.

The Parties recognize the critical importance of protecting health data and commit to adhering to all relevant legal and regulatory standards, including the EU General Data Protection Regulation (EU GDPR), the French Data Protection Act, and HDS certification guidelines, as released from time to time. This Addendum formalizes the parties' shared commitment to ensuring the secure management of health data within a compliant framework.

1. Definitions

For the purposes of this Addendum, (i) "**Health Data"** means health data contained in the Customer Data and defined by Article L. 1111-8 of the French Public Health Code (FPHC), i.e. personal health data collected in the course of prevention, diagnostic, care or social or medico-social activities, and (ii) "**Hosting Service**" means the performance of the activities listed from points 3° to 6°of Article R. 1111-9 of the FPHC by Genesys, described hereafter in clause 2.

2. Conformity Certificate

2.1. Genesys is a certified Health Data Hosting Service provider within the meaning of Article L. 1111-8 of the FPHC for the activities listed from point 3° to 6° of Article R. 1111-9 of the FPHC, namely:

- Making available and maintaining in an operational condition the virtual infrastructure of the information system used to process health data;
- Making available and maintaining in an operational condition the information system application hosting platform;
- Administrating and operating of the information system containing the health data; and
- Backing up the Health Data.

2.2. The certification of compliance was delivered under No. FR22/00000045 on 13 September 2022 by SGS ICS France (the "**Certification**") for a renewable duration of three (3) years, to be renewed by 12 September 2025.

2.3. Genesys shall provide the Customer with a copy of the HDS certification, including the certificates of processors involved in the hosting activities where applicable. The certificate of compliance and the related audit reports are available for consultation upon request from the Customer at Genesys' premises.

3. Scope of Services

3.1. The Services provided by Genesys are described in the Agreement, at https://help.genesys.cloud/solutions-subscription-plans-licensing-and-pricing-home/, or through an applicable Statement of Work, Addendum or Amendment signed in the framework of the said Agreement. The Cloud Services are designed to achieve the service levels described at https://help.genesys.cloud/articles/service-level-agreements/.

3.2. In accordance with Article R. 1111-11, 11° of the FPHC, Genesys undertakes not to use Health Data for any other purposes that those set out in this Addendum, and specifically not for marketing, advertising, commercial or statistical purposes.

3.3. Genesys shall process Health Data and more generally personal data contained in the Customer Data only on documented instructions from the Customer, as provided in the Data Processing Terms Schedule and more particularly in Section 2.d of the Data Processing Terms Schedule.

3.4. The below Health Data Security Responsibility Matrix defines the limits of Genesys' responsibility regarding the scope of security measures to be taken for the safeguarding of Health Data. The organization of the respective responsibilities between Customer and Genesys is done through the definition of a RACI according to the different elements of the service operations:

R = Responsible
Responsible for performing the task (ie. the actual entity doing the work to complete the task).

A = Accountable
Ultimately accountable for the instigation and completion of the task in a satisfactory manner.

C = Consulted
The entity whose input is used to complete the task. Communication with this entity will be 2-way in nature.

I = Informed
The entity who is informed as to the status of the task. Communication with this entity will be 1-way in nature.

The Parties commit to fulfill their respective responsibilities as per the RACI definition and below matrix:

Scope of security measures	AWS	Genesys	Customer
	AWS Region (Data Centers)	Cloud Services Environment	Equipment and Customer's equipment and IT environment
Physical access to the premises and information systems where the Health Data is hosted (AWS Region)	**R / A**	**C**	**I**
Access to the information systems and to the Health Data, in accordance with the security framework referred to in article L. 1110-4-1 of the FPHC and the PGSSI-S, specifically regarding identification and authentication requirements	**I**	**R**	**R / A**
Health Data access traceability	**C**	**R**	**A**
Health Data sharing and exchanging between health professionals, in accordance with the rules applicable to Health Data confidentiality and professional secrecy, specifically as set forth by article L. 1110-4 of the FPHC	**C**	**R**	**A**
Integrity, security and confidentiality of the Health Data processed by the Cloud Services	**R**	**A**	**C / I**
Availability and backup of the Health Data processed by the Cloud Services	**R**	**R / A**	**C / I**
Information of Data Subjects in accordance with Privacy Legislation	**I**	**C / I**	**R / A**
Management and communication relating to Data Subjects requests as provided under the Privacy Legislation	**I**	**R/ I**	**R / A**
Notification to the Customer in the event of a data breach pursuant to Section 5.a of the Data Processing Terms Schedule	**R**	**A / R**	**I**
Notification to relevant authorities and Data Subjects in the event of a data breach	**C**	**R**	**R / A**

4. Hosting Location

4.1. All Health Data hosting acvities in the context of the Agreement, will be handled within the European Economic Area (EEA). Any remote access outside the EEA shall comply with the applicable transfer formalities as per the GDPR, including adequacy decisions or applicable transfer mechanisms supported by additional safeguards, and transfer mappings will be made available to the Customer on request. Supplementary measures may be added as an amendment to this Addendum or through the applicable Statement of Work.

4.2. Upon Customer's decision, the Health Data is specifically hosted in one of the following AWS Region:

EU (Frankfurt)	eu-central-1	EMEA (Frankfurt)	https://login.mypurecloud.de
Europe (Ireland)	eu-west-1	EMEA (Dublin)	https://login.mypurecloud.ie

The Customer hereby assumes its responsibilities in respect to choosing the appropriate hosting location in fulfiment of its regulatory obligations and contractual commitments under this Addendum and the Agreement.

In addition to the above, the Health Data may be hosted in a Backup AWS Region in the event that the relevant customer purchases a Disaster Recovery package from Genesys.

5. Data Subjects' Rights

5.1. The Customer is responsible for providing Data Subjects with the information they are entitled to receive in relation to the processing of their Health Data and for answering Data Subjects requests to exercise any of their rights, including their rights of access (subject to Clause 8 of Appendix 1 of the Data Processing Terms Schedule), rectification, erasure or opposition, right to restriction of processing, right to data portability, right not to be subject to automated individual decision-making (including profiling) in accordance with Chapter III of the GDPR, their right to object under Article L. 1111-8 of the FPHC, as well as their right to access medical records under Article L. 1111-7 of the FPHC.

5.2. As per Section 2.h of the Data Processing Terms Schedule and Clause 8 of Appendix 1 of the Data Processing Terms Schedule, in the event Genesys receives requests from Data Subjects, Genesys shall forward such requests to the Customer and provide the Customer with assistance in the performance of its obligations.

6. Security

6.1. Genesys ensures the security of the Cloud Services Environment as set forth in its security policy located at https://help.genesys.cloud/articles/genesys-cloud-security-policy/, and will make sure to provide the appropriate technical and organizational measures for the data processing activities carried out in the context of this Schedule, as set forth in Section 3.b of the Data Processing Terms Schedule.

6.2. Considering its scope of responsibility as described in Section 3 of this Schedule, the Customer acknowledges that it must comply with the security framework referred to in article L. 1110-4-1 of the FPHC, and specifically to the General Security Policy for Health Information Systems ("*PGSSI-S*") published by the French Digital Health Agency ("*Agence du Numérique en Santé*") and shall undertake to do so by completing the certificate provided in Exhibit 1.

7. Data Breaches

7.1. Genesys shall notify the Customer as soon as possible after becoming aware of any data breach pursuant to Section 5.a of the Data Processing Terms Schedule and attach a description of the breach to this notification, including where possible, the date on which the breach was discovered, the scope of the breach, the compromised information systems, the source of the breach and the status of the breach management.

7.2. For the above purpose, the Customer provides herein the identity and contact details of the person that Genesys must notify in the event of such a breach:

Name:

Email:

Telephone:

The Customer shall notify in writing to Genesys any modification of the above point of contact and place a request to change the point of contact to Genesys Support.

7.3. The above point of contact shall be able to provide Genesys with the name of a health professional, whenever necessary.

8. Audits

8.1. As per Sections 3.c.ii and 4 of the Data Processing Terms Schedule, Genesys undertakes to make available to the data protection officer of the Customer and to any competent supervisory authority the documentation necessary to demonstrate compliance with the obligations set out in this Schedule and with its legal obligations regarding the hosting of Health Data under articles L. 1111-8 *et seq.* and R. 1111-9 *et seq.* of the FPHC that are under Genesys responsibility, as set forth in this Schedule.

8.2. Customer may conduct or commission audits on dedicated resources, access logs for systems used to process Health Data, and summaries of independent audits conducted on shared resources within the previous three (3) years.The conditions applicable to these audits, are set out in Section 4 of the Data Processing Terms Schedule and may be supplemented by the relevant terms in the Technical and Organisational Measures.

9. Service continuity procedures

Genesys shall implement the business continuity and operational resilience procedures set out in Attachment 2 of the Data Processing Terms Schedule. In addition to the above, the applicable Service Level Agreements set out in the Agreement will stay as a reference in relation to Genesys ability to continue rendering a persistent health data hosting service as well as to set out the conditions for the recovery and its inherent commitments.

10. Subcontracting

10.1. Genesys shall be entitled to subcontract all or part of the Services, subject to Section 6 of the Data Processing Terms Schedule for all subcontractors involved in the processing of personal data and in particular Health Data ("**Subprocessor**"), and provided that (i) such Subprocessors shall ensure the same level of undertakings as set out in this Schedule, and (ii) Genesys shall remain liable to the Customer for the observance and performance of its obligations under this Schedule and more generally under the Agreement.

10.2. Genesys will ensure its Subprocessors maintain updated Technical and Organizational Measures to mitigate risks as per Health Data Hosting certification standards, and inform the Customer of significant changes impacting service delivery or compliance.

10.3. The list of Subprocessors used by Genesys on the date of signature of this Agreement is attached in Annex IV of Attachment 1 of the Data Processing Terms Schedule. Any change to such Subprocessors is subject to Section 6 of the Data Processing Terms Schedule: in particular, at least 30 days prior to engaging a new Subprocessor, Genesys will update the List of Subprocessors and notify the Customer by sending a message to the email address then associated with the Customer's account.

11. Access to Health Data

11.1. Access to Health Data shall be controlled by Genesys as set out in Section 7.5 of Appendix 1 of the Data Processing Terms Schedule.

11.2. The Customer undertakes (i) to formalize, implement and regularly audit the remote access control procedure, in particular, without limitation, in accordance with the Technical and Organisational Measures included in the Data Processing Terms Schedule, as well as in accordance with the instructions laid down by Customer in Annex II of the above mentioned Data Processing Terms; (ii) to comply with the rules applicable to Health Data confidentiality and professional secrecy, specifically the requirements applicable to Health Data exchange and sharing, as set forth by article L. 1110-4 of the FPHC, and (iii) to comply with the requirements set out by the security framework referred to in article L. 1110-4-1 of the FPHC, in particular regarding identification and authentication requirements.

11.3. The Customer acknowledges that governmental or court-ordered seizure proceedings targeting the Customer's data located in the Cloud Service Environment may occur, in accordance with applicable law. Should Genesys be informed that such proceedings are being initiated, Genesys shall notify the Customer of such proceedings upon receipt of the seizure request, unless said request or applicable law forbids such notification. Genesys shall keep records of such proceedings, including, if applicable, the targeted data, the requesting judicial or governmental authority and the date of the proceedings.

12. Additional Termination Rights

In addition to the termination rights set out in the Agreement, the Customer may immediately terminate this Agreement without payment of compensation or indemnification to Genesys for any damage caused by such termination, by giving written notice to Genesys if the Certification is not renewed by Genesys or withdrawn or lost, provided that such withdrawal or loss is due to Genesys 's exclusive fault. Likewise, upon termination of the Agreement, Genesys commits to return all Health Data to the Customer, to destroy any remaining copies, and outline the reasonable fees, if applicable, and timeframes for these actions, if applicable. Data shall be returned in a format suitable for portability.

13. Agreement with the data controller

The Customer shall ensure that its agreement with the data controller of the Health Data, if different from the Customer, for the provision of services related to the processing and hosting of Health Data complies with and reflects the requirements of Article R. 1111-11 of the French Public Health Code and this Agreement, in particular this Schedule.

Exhibit 1: Certificate of Compliance with the PGSSI-S

EXHIBIT 1

Certificate of Compliance with the PGSSI-S

Customer	**[** **]** (with share capital of €[ ] and incorporated under number [ ])
Customer's Address	[ ]

The Customer acknowledges that it is subject to compliance with the provisions of the security framework referred to in article L. 1110-4-1 of the FPHC, and specifically to the General Security Policy for Health Information Systems ("***PGSSI-S***") published by the French Digital Health Agency ("*Agence du Numérique en Santé*"), that are applicable to the Customer with regard to its activities within the health and medico-social sector.

The Customer, having read and understood the terms of the PGSSI-S, declares that it is in compliance with the provisions that are applicable to its activities within the health and medico-social sector. The Customer undertakes to remain in compliance with the provisions of PGSSI-S, including with the possible amendments made to the PGSSI-S at any time. The Customer undertakes to remind the data controller (if different from the Customer) to comply with the PGSSI-S to extent applicable to its activities.

The Customer acknowledges that in the event of non-compliance with the provisions of the PGSSI-S, it is liable to the sanctions provided for by Article 83 of the GDPR. Genesys shall not be held liable for non-compliance of the Customer with the provisions of PGSSI-S regarding the Customer's activities within the health and medico-social sector.

The Customer shall ensure that its employees, and subsequent data processors if appointed, have committed themselves to comply with the PGSSI-S provisions.