GENERAL TERMS AND CONDITIONS OF KLINEO SERVICES – DOCTORS

As of 17.02.2026

KLINEO is incorporated as a simplified joint stock company (S.A.S.) with capital of €19,095.58, registered with the NANTERRE Trade and Companies Register under number 904 525 706, with its registered office located at 6, rue des Bateliers, 92110 CLICHY, France, and its intra-community VAT number is FR93904525706. The KLINEO Platform enables: - Patients undergoing oncology treatment and their referring physicians to identify clinical trials that may offer a therapeutic option for patients. - Investigators to preselect patients whose profiles meet the inclusion criteria for the clinical trial they are responsible for. The purpose of the KLINEO Terms and Conditions of Service (hereinafter the "T&Cs") is to define the terms and conditions of the Services provided by KLINEO to Referring Physicians and Investigators under this agreement (hereinafter "the Agreement"), as well as their respective rights and obligations. They are available in PDF format at any time at the bottom of the Platform. The terms used in these GTC with capital letters are defined here .

The Services are provided to Physicians free of charge.

Table of contents

1. DEFINITIONS

The definitions attached to these GTC are available here.

2. HOW DOES KLINEO WORK?

2.1. REFERENCING OF CLINICAL TRIALS

The KLINEO Platform (https://www.klineo.fr/) references clinical trials currently being enrolled in France that are available on public sources, including clinicaltrial.gov, CTIS, etc.

Referring physicians and patients can use an anonymous form to search for clinical trials on the platform that match the patient's therapeutic needs by entering clinical criteria.

The order in which query results are displayed depends on:

- the relevance of the trial based on the clinical criteria met (e.g., type of cancer, histological type, presence or absence of a biomarker, etc.),
- the geographical distance from the location provided,
- updating of data by the Sponsor (e.g., status of the investigational site opening).

2.2 CREATION OF AND ACCESS TO PATIENT MEDICAL RECORDS

The Patient Medical Record can be created by the Patient in accordance with the CGS Patients or by their Referring Physician under the conditions set out in Article 4.2 hereof.

The Patient Medical Record is accessible exclusively:

- to the Patient via their Patient Account,
- to the Referring Physician via their Referring Physician Account.
- to any Investigating Physicians with whom the Referring Physician would share it
- to KLINEO's medical and technical teams to ensure the smooth running of all KLINEO services.

The Patient Medical Record can only be modified:

- by the Patient,

- by the Referring Physician.

Investigating Physicians only receive a non-editable version of the Patient Medical Record, which is up to date at the time it is sent by the Referring Physician.

The Patient and the Referring Physician have shared access to the Patient Medical Record via their respective Patient and Physician Accounts.

They can both access, modify, add to, or delete any information or document contained in the Patient Medical Record.

In the event of modification and/or deletion of information or a document by the Referring Physician, the information or document is automatically modified or deleted from the Patient Medical Record accessible to the Patient.

Similarly, if the Patient modifies or deletes any information or document, the information or document is automatically modified or deleted from the Patient Medical Record accessible to the Referring Physician.

KLINEO is in no way responsible for the content, accuracy, or updating of information and/or documents recorded or shared on the Patient Medical Record by the Patient or the Referring Physician.

The Referring Physician undertakes to keep the Patient Medical Record up to date and, where applicable, to update it before sharing it with the Investigating Physician in order to ensure that the Patient Data contained therein is accurate at all times.

2.3 COMMUNICATION WITH A CLINICAL TRIAL INVESTIGATOR

In order to benefit from KLINEO's Services and enable their Patients to benefit from them, the Referring Physician must create a Physician Account in accordance with Article 3.

The Patient may create a Patient Account in order to complete their Patient Medical Record and indicate clinical trials to their Referring Physician, but they are not authorized to send their Patient Medical Record to an Investigating Physician or to communicate with the latter.

Only the Referring Physician may communicate with an Investigating Physician and send them the Patient Medical Record.

In the case of a partner trial, the Referring Physician can contact the Investigator in charge of the clinical trial directly on the Platform. In the case of a non-partner trial, the Referring Physician can contact the center where the trial is being conducted using publicly available information.

If the Patient Medical Record meets the clinical trial screening criteria, the Investigator informs the Referring Physician.

The Referring Physician then informs the Patient of their pre-selection so that they can arrange a consultation appointment with the Investigating Physician for the clinical trial, who will ensure that the Patient's profile meets the trial criteria.

The KLINEO Platform thus enables the preselection of clinical trials for which patient profiles meet the inclusion criteria of the referenced clinical trials.

The KLINEO Platform compiles aggregate statistics on the use of these services, including user activity, clinical trials, and their inclusion criteria. These statistics are anonymous and may be included in the services offered to Klineo's partners.

Pre-selection does not in any way prejudge the final decision on inclusion, nor does it replace appointments, examinations, or medical explanations by the Investigating Physician regarding inclusion, the scope, risks, and consequences of the Clinical Trial, which will be carried out by the Investigating Physicians outside the Platform and under their sole responsibility, in accordance with applicable regulations.

The Patient is always free to accept or refuse to participate in any clinical trial that may be offered to them.

3. CREATING A DOCTOR ACCOUNT

3.1. CONDITIONS OF ACCESS

The creation of a Physician Account is reserved for healthcare professionals with an RPPS number.

These GTC, as well as KLINEO Privacy Policy, must be read and accepted by the Physician when creating their Physician Account.

3.2 ACCOUNT INFORMATION

When creating their account, doctors are asked to log in via their Pro Santé Connect space.

If the Physician does not have a Pro Santé Connect account, they are asked to provide the following information: Last name, First name, Work address, Email, Mobile phone number, Gender, Name of center, RPPS/e-CPS number, Medical specialty.

The Physician undertakes to keep the information provided in their Physician Account up to date and, where necessary, to update it immediately to ensure that it remains accurate at all times.

In the event that the Physician provides false, inaccurate, obsolete, incomplete, or misleading information, KLINEO may suspend access to the Physician Account and deny the Physician access, temporarily or permanently, to all or part of the Services.

Pour en savoir plus sur le traitement par KLINEO de ses Données Personnelles, le Médecin est invité à consulter la Politique de confidentialité disponible here et à tout moment en pied de page de la Plateforme.

3.3. TECHNICAL SPECIFICATIONS FOR ACCESSING SERVICES

The Physician's Account is accessible via login credentials chosen by the Physician, which meet the security standards set by KLINEO and are linked to a two-factor authentication system. The Physician undertakes to keep these credentials confidential and not to disclose them in any form whatsoever.

The Physician is solely responsible for the use made of his/her Login Details. Any access to, use of the Services, and transmission of Physician Data or Patient Data made from the Physician Account will be considered to have been made by the Physician.

The physician is solely responsible for providing his or her login details to third parties, including assistants, ARC staff, and nurses.

Any loss or misappropriation of a Physician's login details and the consequences thereof are the sole responsibility of the Physician.

In the event of loss or misappropriation, the Physician is required to notify KLINEO immediately at support@klineo.fr so that KLINEO can reset and/or suspend the Patient Account.

4. SERVICES RELATED TO THE REFERRING PHYSICIAN ACCOUNT

Through their Account, the Referring Physician can:

- access a Patient Medical Record already completed by the Patient on their Patient Account (see section 4.1).
- complete a Patient Medical Record himself after obtaining the Patient's consent and duly informing him of his rights (see Article 4.2)
- send a Patient Medical Record to one or more Investigating Physician(s) participating in the selected clinical trial (see Article 4.3).

4.1 ACCESS TO A PATIENT MEDICAL RECORD PRE-FILLED BY THE PATIENT

The Referring Physician can access the Medical Record of a Patient who has listed them as their Referring Physician on their Patient Account.

The Referring Physician can thus access, modify, add to, or delete any information or document contained in the Patient Medical Record.

In the event of modification and/or deletion of information or a document by the Referring Physician, the information or document is automatically modified or deleted from the Patient Medical Record accessible to the Patient.

4.2 CREATION OF THE PATIENT MEDICAL RECORD BY THE REFERRING PHYSICIAN

As part of the care provided to their oncology patients, referring physicians may suggest that their patients use the KLINEO platform to identify clinical trials that could offer a treatment option for them.

The Referring Physician can create a Patient Medical Record himself, based on the Patient Data collected and stored as part of his Patient's medical follow-up.

When creating the Patient Medical Record on KLINEO, the Physician undertakes to have previously:

- **obtained the Patient's consent for the transfer of their Patient Data to KLINEO,**
- **obtained the Patient's consent to share this form with one or more Investigating Physicians**
- **and duly informed them of their rights by providing them with the Patient Information Sheet made available by KLINEO, which can be printed directly from the Physician Account (specify tab).**

4.2.1. Manual creation

When creating the Patient Medical Record, the Referring Physician is asked to provide all or part of the following information about the Patient: Type of cancer (affected organ, histology, biomarker, medical reports, biological reports, medical imaging reports), medical history, fitness level (independence, etc.).

The Referring Physician may attach documents to it, including medical reports, laboratory reports, and medical imaging reports.

If the Patient subsequently creates a Patient Account, they will be able to access, modify, complete, or delete any information or documents contained in the Patient Medical Record completed by the Referring Physician.

4.2.1. Creation via artificial intelligence

Klineo offers an AI-powered record creation module that automatically extracts and structures patient medical data to facilitate matching with referenced clinical trials. This structuring aid enables fast, accurate, and robust searching.

All operations are performed on HDS-certified environments. Only pseudonymized or anonymized data can be used to train the models.

The textual content of medical reports is extracted (using OCR if necessary) and then structured to highlight the relevant clinical data.

Each structure generated by AI is systematically presented to the user for validation. The user can modify it freely at any time, including after saving. No automatically extracted information is used without human validation.

A monitoring system detects any significant deviation from expected behavior. All changes to the system are rigorously evaluated using representative data sets and are documented to ensure the traceability of developments.

The Referring Physician undertakes to keep the Patient Medical Record up to date and, where applicable, to update it before sharing it with the Investigating Physician in order to ensure that the Patient Data contained therein is accurate at all times.

4.3. SENDING A PATIENT MEDICAL RECORD TO AN INVESTIGATOR PHYSICIAN

4.3.1. Selection of the clinical trial

The Referring Physician can search for a clinical trial using an anonymous form or the Patient Medical Record.

Patients also have the option of searching for and sharing a clinical trial with their Referring Physician.

In both cases, the Referring Physician shall assess, **under his or her sole responsibility**:

- the relevance of the identified clinical trial in relation to the therapeutic needs of his/her patient;
- the opportunity to send the Patient Medical Record to one or more Investigating Physicians in charge of the clinical trial, taking into account the Patient's profile.

4.3.2. Communication with the Investigator

To send a Patient Medical Record to an Investigating Physician, the Referring Physician can contact them via KLINEO's secure messaging system and attach a non-editable copy of the Patient Medical Record.

Investigating Physicians receive only a non-editable copy of the Patient Medical Record, which is up to date at the time it is sent by the Referring Physician.

Once the Patient Medical Record has been sent to an Investigating Physician, the Referring Physician undertakes to immediately inform them of any changes to the Patient Data, including Health Data, in order to ensure that it remains accurate at all times.

5. SERVICES RELATED TO THE INVESTIGATOR ACCOUNT

Through their Account, the Investigating Physician can:

1. receive the Patient Medical Record sent by the Referring Physician (see Article 5.1).
2. notify the Referring Physician of the decision to pre-select the Patient for the trial (see Article 5.1)
3. access a table tracking the preselection of patients (see Article 5.2)

5.1 RECEIPT OF A PATIENT MEDICAL RECORD SENT BY THE REFERRING PHYSICIAN

When a Patient Medical Record is received from a Referring Physician, the Investigating Physician receives a notification via the secure KLINEO messaging system and, if desired, by email.

He can then consult the copy of the Patient Medical Record received, in order to determine whether the Patient's profile meets the inclusion criteria for the clinical trial in which he is participating.

He can communicate with the Referring Physician via the secure KLINEO messaging system to request additional information.

The Investigator undertakes to examine the Patient Medical Record received **with the utmost care** and to inform the Referring Physician of his/her positive or negative decision on pre-selection as soon as possible.

In the event of a pre-selection decision, the Investigator then undertakes to comply with the clinical trial selection protocol, **and in particular to arrange a consultation with the Patient for the purpose of informing them of the scope, risks, and consequences of the Clinical Trial and to carry out all necessary examinations and checks, under their sole responsibility, in accordance with applicable regulations.**In order to arrange this consultation, the Investigator may share their contact details (email address and telephone number) with the Referring Physician.

The Investigator's decision to preselect a patient does not in any way prejudge the final decision on inclusion, which will be made after consultation with the Patient.

The Patient is always free to accept or refuse to participate in any clinical trial that may be offered to them.

1. ACCESS TO A PRE-SELECTION TRACKING TABLE

The Investigator also has access to a table summarizing the number of Patient Medical Records received for the clinical trial.

The Investigator undertakes to inform the Referring Physician, for a pre-selected Patient, whether or not the Patient has been included in the clinical trial, so that the Referring Physician can take this information into account when treating and monitoring their Patient.

6. MODIFICATION OF THE PLATFORM, SERVICES, OR TERMS AND CONDITIONS

KLINEO may modify all or part of the Platform, Services, and GTC at any time.

In the event of a significant change to the Platform, the Services, or the GTC, KLINEO will inform the Physician by email notification and with reasonable notice, lasting a minimum of 15 (fifteen) days.

A shorter notice period or no notice period may nevertheless apply in the event that the modification of the Services is necessary due to a change in the legal and/or regulatory obligations incumbent upon KLINEO or that such modifications are imposed by the need to deal with an unforeseen and imminent danger in order to protect Patients, KLINEO, and/or third parties. KLINEO, and/or third parties.

Physicians may terminate their Contract under the conditions set forth in Article 12.

If the Contract is not terminated within the notice period, changes to the Platform and/or Services and/or GTC shall be deemed to have been accepted by the Physicians.

The changes shall take effect at the end of the specified notice period.

7. DURATION OF SERVICES

Creating a Physician Account on KLINEO gives them access to the following Services:

- until termination of the Contract by KLINEO or by the Physician under the conditions set forth in Article 12.1 or 12.2;
- or, failing that, until the expiry of a period of two (2) years from the last activity on the Physician Account in accordance with Article 12.3.

The Referring Physician undertakes to delete the Patient Medical Records that he/she has completed in accordance with the conditions set out in Article 4.2 as soon as he/she becomes aware of:

- **the Patient's disagreement with the transfer of their Patient Data to KLINEO;**
- **or, more generally, any other cause that would prevent it from retaining Patient Data or transmitting it to KLINEO.**

The Referring Physician also undertakes to immediately inform KLINEO of the Patient's decision to change Referring Physicians.

8. KLINEO'S OBLIGATIONS AND RESPONSIBILITIES

KLINEO makes every effort, in accordance with the state of the art, to ensure the smooth operation and continuity and quality of the Services.

The Physician acknowledges that the KLINEO Platform is intended to meet the needs of the greatest number of people and not to adapt to any particular requirement on his or her part.

The Physician acknowledges that KLINEO cannot be held liable for any interruption of Services beyond its control and, in particular, that the provision of Services depends on the reliability, availability, and continuity of third-party connections (telecommunications network operators, Internet, etc.). KLINEO may be required to suspend the Services for maintenance purposes and/or in the event of technical requirements. It will endeavor to inform users in advance and to schedule such maintenance operations outside of business hours.

It is understood between the Parties that KLINEO shall not be held liable for any indirect damages suffered by the Physician in connection with the use of the Services.

KLINEO declines all responsibility in the event of a dispute, regardless of the cause, between Doctors or between a Doctor and a Patient or third-party partner, which is not attributable to KLINEO.

The Physician acknowledges that KLINEO's role is limited to that of a simple intermediary and technical service provider.

KLINEO is in no way responsible for the content, accuracy, or updating of information or documents recorded or shared by the Physician on their Physician Account, or by the Patient on their Patient Account.

KLINEO does not provide any medical advice on clinical trials, which are listed according to criteria defined by the sponsors and which the latter have chosen to communicate to KLINEO.

The decision to send the Patient Medical Record to one or more Investigating Physicians is made exclusively by the Referring Physician, under his or her sole responsibility. The Referring Physician is solely responsible for monitoring Patient Medical Records that are pending.

Consultation regarding information on the clinical trial, obtaining consent, and inclusion in a clinical trial is carried out by the Investigating Physicians outside the KLINEO Platform and under their sole responsibility, in accordance with applicable regulations. The Patient is always free to accept or refuse to participate in a clinical trial that may be offered to them.

Consequently, KLINEO cannot under any circumstances be held liable (i) for the content of any information or document recorded on KLINEO by the Patient or a Physician, (ii) for the inclusion or non-inclusion of a Patient in a clinical trial, (iii) for the effects and consequences of participation in a clinical trial for the Patient.

9. OBLIGATIONS AND RESPONSIBILITIES OF THE PHYSICIAN

The Physician undertakes to:

- comply with the terms of these GTC;
- verify that they have the necessary equipment to use the Services, in particular technical equipment and an Internet access network;
- protect yourself against the risks of loss and/or hacking of data, files, and programs, in particular by using regularly updated antivirus software packages;
- secure its methods of access to the Services in order to prevent unauthorized use of the Services;
- use the Services in compliance with the laws and regulations applicable to the GTC;
- not to use the Services in a manner that could damage the reputation of KLINEO and/or other users of the Platform;
- use the Platform and Services for professional purposes;
- indemnify KLINEO for all costs (including legal fees, costs, and expenses) and damages related to claims and legal actions arising from your violation of any provision of the GTC.

The Referring Physician specifically undertakes to:

- provide KLINEO with all information necessary for the provision of the Services.
- verify that the Patient Medical Record is complete and up to date.
- In the event of a Patient Medical Record being sent to an Investigating Physician, the Referring Physician shall be solely responsible for the consequences of any failure or delay in updating the Patient Data in the Patient Medical Record. **The Referring Physician undertakes to immediately inform the Investigating Physician of any changes to the Patient Data that may affect the patient's eligibility for a clinical trial.**

The Investigator undertakes in particular to:

- Take all necessary care in reviewing the Patient Medical Records sent to them as soon as possible.
- Inform the Referring Physician of the outcome of a Patient's pre-selection as soon as possible.
- In the event of a decision not to select a subject, the Investigator undertakes to inform the Referring Physician of the reasons for non-selection, subject to any professional confidentiality obligations relating to the ongoing clinical trial.

10. COMMUNICATION ABOUT KLINEO SERVICES AND NEWS

By creating a Doctor Account and entering their email address, Doctors authorize KLINEO to send them internal messages on the Platform and emails relating to KLINEO's services and news, including:

- For the Referring Physician: new clinical trials that may be of interest to them based on the Patient Medical Records linked to their Physician Account and/or, more generally, their specialty and geographic area.
- For the Investigator: notifications regarding Patient Medical Records received.

The Physician may opt out of receiving internal messages and/or emails at any time in their Physician Account.

11. INTELLECTUAL PROPERTY

KLINEO Services and all elements comprising them are, unless otherwise specified, the exclusive property of KLINEO.

KLINEO grants the Physician, for the duration of the Agreement, a personal, non-exclusive, non-assignable, and non-transferable right to use the KLINEO Platform.

KLINEO reserves all rights, including the right to correct or modify any Service. This Agreement does not grant the Physician any ownership rights in relation to the Platform, the Services, their technology, or the intellectual property rights held by KLINEO or any third party.

The Physician is prohibited from interfering in any way with the KLINEO Platform or Services, and in particular from using the Services in a manner that does not comply with their intended purpose and the conditions set out in the GTC. Consequently, the Physician:

- shall refrain from attempting to access or copy the source codes and/or data of the KLINEO Platform;

- shall refrain from creating a competing product or service and/or copying or reproducing any features, functions, or graphic attributes of the KLINEO Platform or Services.

- agrees not to distribute the Services or make them available to third parties.

- agrees not to alter or disrupt the integrity or performance of the Services or the data contained therein.

- agrees not to attempt to gain unauthorized access to the Services or to the systems or networks associated with them.

The Physician assumes full responsibility for the nature, content, accuracy, integrity, and legality of the Physician Data and Patient Data transmitted by him/her to KLINEO in connection with the Services, as well as for the use thereof.

The Physician acknowledges that any violation of this article may be subject to civil and/or criminal penalties in accordance with the law and these GTC.

12. SUSPENSION OF THE DOCTOR'S ACCOUNT

In the event of non-compliance by the Physician with the provisions of the Contract, the law, and/or applicable regulations that may cause harm to KLINEO, a Patient, another Physician, or a third party, KLINEO may give formal notice to the Physician to remedy the breach(es) within seven (7) days of the date of notification.

If the Physician fails to comply with its obligations within this period, KLINEO may also automatically suspend or restrict the Physician's access to all or part of the Services.

In the event of particularly serious non-compliance, such as identity theft or abusive or malicious use of the Platform's features, KLINEO also reserves the right to suspend or limit the Physician's access to all or part of the Services **without prior notice.**

Unless resulting from a fault on its part, KLINEO shall in no event be held liable for any damage resulting from the suspension of the Services.

12. TERMINATION OF THE AGREEMENT

12.1 TERMINATION BY THE DOCTOR

The Physician may terminate their Contract at any time by requesting the deletion of their Physician Account at support@klineo.fr or via their Physician Account.

The termination request will take effect within a maximum period of one (1) month from the date of receipt.

12.2 TERMINATION BY KLINEO

KLINEO may terminate all or part of the Services offered at any time, without having to justify its decision and without compensation.

In this context, the Physician is informed that KLINEO must give fifteen (15) days' notice.

12.3 AUTOMATIC TERMINATION IN CASE OF INACTIVITY

In the event of inactivity on the Physician Account for a period of two (2) years and after a termination notice sent by email has remained unanswered, the Physician Contract will be automatically terminated by KLINEO. At the end of the contract, the data will be pseudonymized and then stored for two (2) years in an archive database for the purpose of improving the algorithm and the patient journey.

This measure is intended to protect the Physician Data and Patient Data entered by the Referring Physician in accordance with data protection regulations and the KLINEO Privacy Policy available here.

12.4 CONSEQUENCES OF TERMINATING A DOCTOR ACCOUNT

Any termination of the Contract shall result, within a maximum period of one (1) month from the effective date of termination, in:

- the termination of the Physician's right to access the Services;
- the deletion of the Physician Account;
- the deletion of Patient Medical Records present in the Physician Account;
- the deletion, archiving, or anonymization of Physician Data or Patient Data in accordance with the Privacy Policy.

In accordance with their right to data portability, physicians who submit a written request may retrieve their data in CSV, Excel, or PDF format before their physician account is deleted.

13. NOTIFICATIONS

Unless otherwise specified, notifications made under the GTC shall be sent either by email or by any other means that provides proof of receipt.

For the purposes of these GTC, the Physician acknowledges that the postal and email addresses provided in their Physician Account shall serve as the reference for sending any notifications pursuant to these GTC.

KLINEO elects domicile and may receive notifications at the following addresses:

-By mail: 6, rue des Bateliers, 92110 CLICHY.

-By email: info@klineo.fr

14. PERSONAL DATA

The Personal Data Protection Policy available at KLINEO.com describes the respective roles and obligations of the Healthcare Professional and KLINEO regarding the processing of Personal Data in connection with the performance of the Services.

By accepting these GTC, the Healthcare Professional and KLINEO undertake to comply with the terms and conditions of this personal data protection policy.

14.1 SUBCONTRACTING AGREEMENT

When a healthcare professional who uses the KLINEO Platform creates and manages their patient's medical record, they are considered to be the "Data Controller" and KLINEO is considered to be the data processor for the Healthcare Professional or the Hospital where the Healthcare Professional works, in accordance with the provisions of the General Data Protection Regulation ("GDPR") of April 27, 2016. In cases where the Hospital Centre is

responsible for processing, the healthcare professional must submit the data processing agreement in Appendix 1 of the new version of the GTC for signature by the Chief Executive Officer or the DPO of their institution. Within the framework of their contractual relations, the parties undertake to comply with the regulations in force applicable to the processing of personal data and, in particular, Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter, "the European Data Protection Regulation").

In this context, the subcontractor is authorized to process, on behalf of the Data Controller, the personal data necessary to provide the KLINEO Platform, enabling healthcare professionals to create patient medical records and allowing patients to be included in clinical trials in order to provide them with a treatment option.

The processing operations performed by the subcontractor on the data are:

X Pseudonymization		
☐ Collect	☐ Modification	☐Reconciliation
X Lecture	☐ Extraction	or interconnection
☐ Ranking	X Transmission	☐ Limitation
X Recording	☐ Diffusion	X Erasure or
X Conservation/archiving		destruction

The categories of persons concerned are:

- Healthcare Professionals
- Patients treated by these healthcare professionals

The personal data of the data subjects processed are:

- Healthcare professionals: personal identification data, data concerning professional life, contact details.
- Patients treated by these healthcare professionals: personal identification data, contact details, health data, genetic data, where applicable.

The retention period for personal data by the processor is:

- two years on active duty as part of the service,
- Then, after two years of inactivity on the professional health account or at the end of the contract, the data is pseudonymized and stored in an archive database for a period of two years.

In any event, the subcontractor shall retain the data processed during the provision of services for the duration of the agreement concluded between it and the data controller. The subcontractor is responsible for the necessary technical and organizational measures it implements to comply with the principle of minimizing the processing of personal data in the context of data retention.

14.1.1 KLINEO's obligations as a subcontractor. The subcontractor undertakes to:

I. process data solely for the purpose(s) for which it is being processed;

II. process the data in accordance with the documented instructions of the Data Controller set out in the appendix to this contract. If the processor considers that an instruction constitutes a breach of the European data protection regulation or any other provision of Union law or Member State law relating to data protection, it shall immediately inform the Data Controller. Furthermore, if the processor is required to transfer data to a third country or to an international organization under Union law or the law of the Member State to which it is subject, it shall inform the Controller of this legal obligation prior to processing, unless the relevant law prohibits such information on important grounds of public interest;

III. alert the Data Controller in writing to their contact email address of any instructions that do not comply with the law and regulations;

IV. ensure the confidentiality of personal data processed under this contract;

V. ensure that persons authorized to process personal data under this contract:

- undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality;
- receive the necessary training in the protection of personal data.

VI. take into account, with regard to its tools, products, applications, or services, the principles of data protection by design and data protection by default.

14.1.2 Obligations of the Healthcare Professional as Data Controller. The Data Controller is required to fulfill its obligations under the GDPR, in particular with regard to the obligation to inform data subjects about processing operations at the time of collection of personal data, the maintenance of a record of processing activities, and more generally, compliance with the principles set out in the GDPR.

The Data Controller further undertakes to:

- allow healthcare professionals to provide the processor with the personal data referred to in the processing characteristics in connection with their use of Klineo;
- document in writing any instructions concerning the processing of personal data by the processor;
- ensure, prior to and throughout the duration of the processing, that the processor complies with the obligations set out in the European data protection regulation;
- supervise the processing, including conducting audits and inspections of the subcontractor, if deemed necessary.

14.1.3 Exercise of individuals' rights. To the extent possible, the Processor shall assist the Controller in fulfilling its obligation to respond to requests from data subjects to exercise their rights: right of access, rectification, erasure, and objection, right to restriction of processing, right to data portability, right not to be subject to automated individual decision-making (including profiling). When data subjects submit requests to exercise their rights to the processor, the processor must, without responding to them, forward these requests upon receipt by email to the contact address provided by the Data Controller.

14.1.4 Notification of personal data breaches. The Processor shall notify the Controller of any personal data breach within a maximum of 72 (seventy-two) hours after becoming aware of it, by email to the contact address provided by the Controller. This notification shall be accompanied by any useful documentation to enable the Data Controller, if necessary, to notify the competent supervisory authority of the breach.

14.1.5 Assistance provided by the Subcontractor to the Data Controller. The Subcontractor shall assist the Data Controller, if necessary in view of the requirements of the supervisory authorities, in particular the Commission Nationale Informatique et Libertés (CNIL), in carrying out data protection impact assessments and prior consultation with the supervisory authority, as provided for in the GDPR.

14.1.6 Security measures. The processor undertakes to implement all technical and organizational security measures in the design of the product(s) supplied to the controller. In this respect, the processor undertakes to take into account the provisions relating to Privacy by Design set out in Article 25 of the General Data Protection Regulation. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks, varying in probability and severity, that the processing presents to the rights and freedoms of natural persons, the processor shall implement appropriate technical and organizational measures in an effective manner and provide the necessary safeguards for the processing in order to meet the requirements of the GDPR and protect the rights of the data subjects.

14.1.7 Disposal of data at the end of the contract. At the end of the Services relating to the processing of Personal Data, the processor undertakes to return all personal data to the Data Controller or, where applicable, to the processor designated by the Data Controller, without applying any additional charges. The Data Controller undertakes to provide the subcontractor with the information necessary to carry out the operation relating to the fate of the data.

In the event that the Healthcare Professional agrees to the storage of data by Klineo for the purpose of improving the algorithm and the patient journey for a specified period of time, Klineo will store the data of the individuals concerned in accordance with the established period (two years) in its capacity as an independent Data Controller for this purpose.

14.1.8 Registre des traitements de données. Le sous-traitant déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du Responsable de Traitement.

14.1.9 Délégué à la protection des données. Le sous-traitant a désigné un Délégué à la data protection in accordance with the provisions of Article 37 of the GDPR.

	The Subcontractor
Contact email	dpo@klineo.fr

14.1.10 Documentation and audit. The Subcontractor shall provide the Data Controller with the necessary documentation to demonstrate compliance with all its obligations and to enable

audits, including inspections, to be carried out by the Data Controller or another auditor appointed by it, and shall cooperate with such audits.

14.1.11 Sub-processors. The Processor shall provide the Controller with the existing list of sub-processors prior to the signing of this Agreement.

The subcontractor must inform the Data Controller of any planned changes in the addition or replacement of its subcontractors, giving the Data Controller the opportunity to object to such changes.

The subcontractor remains fully liable to the Data Controller for the performance, in whole or in part, of the obligations of its subcontractors duly declared and accepted by the Physician.

The subcontractor declares the following subsequent subcontractor(s):
1. BREVO, 106 Boulevard Haussmann, 75008 Paris, France: email marketing solution
2. OVH (OVHCLOUD), 2 RUE KELLERMANN 59100 ROUBAIX: data host

14.1.12 Transfer of data outside the European Union. The processor undertakes to use only means of processing personal data located within the territory of a member country of the European Economic Area and not to transfer personal data to a territory outside the European Economic Area, except in the following cases:
- The transfer is made to a country with an adequate level of personal data protection certified by the European Commission;
- The transfer is made to a company that has joined a specific scheme recognized by the European Commission or, failing that, by the CNIL (French Data Protection Authority).
- The transfer is covered by standard contractual clauses (SCCs) developed by the European Commission.

The subcontractor undertakes to ensure that its affiliates and subcontractors comply with these obligations.

14.1.13 Cooperation with the supervisory authority. Where necessary, the Parties undertake to cooperate jointly in responding to requests from the supervisory authority.

15. EVIDENCE AND EVIDENCE AGREEMENT

Online acceptance of the GTC by electronic means has the same probative value between the Parties as a paper agreement.

16. MISCELLANEOUS PROVISIONS

16.1 - If one or more provisions of the GTC are held to be invalid or declared as such in application of a law or regulation, or following a final decision by a competent court, the other provisions shall remain in full force and effect.

16.2 - Waiver: The failure of either Party to enforce one or more provisions of the Contract shall in no way imply that such Party waives its right to enforce such provisions at a later date.

17. APPLICABLE LAW – DISPUTES

The Contract shall be governed by and construed in accordance with French laws and regulations.

In the event of a dispute relating to the formation, validity, performance, or interpretation of the Contract, KLINEO and the Patient shall endeavor to reach an amicable agreement within thirty (30) days of notification by either party of the need for such an agreement, by registered letter with acknowledgment of receipt.

Except to preserve their right to take legal action or to prevent imminent damage, no legal action may be brought before this amicable dispute resolution procedure has been fully complied with.

In the absence of an amicable agreement, any disputes relating to the validity, application, or interpretation of the Contract shall be submitted to the jurisdiction of the competent courts in accordance with French law.

Appendix 1 (if applicable)

Personal Data Processing Agreement

BETWEEN:

[Name]_____, [Legal form]_____, registered with the Trade and Companies Register under number XXX XXX XXX, whose registered office is located at [Postal address]_____

Hereinafter referred to as “The Client” or the “Data controller”

On the one hand

AND

Klineo, SAS, registered with the Trade and Companies Register under number 904525706, whose registered office is located at bureau 3, 6 rue des Bateliers, 92110 Clichy

Hereinafter referred to as “The Service provider ” or the “Data processor”

On the other hand

Hereinafter individually or collectively referred to as the “Party” or “Parties”

IT HAS BEEN AGREED AND DECIDED AS FOLLOWS:

Definitions

For the purposes of these provisions, the following terms “processing”, “personal data”, “health data”, “person concerned”, “Data controller”, “Data processor”, “record of processing activities”, “personal data breach”, “supervisory authority” within the meaning of the definitions referred to in Article 4 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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 (hereinafter the “GDPR”).

1.1 General provisions. The purpose of these clauses is to define the conditions under which the Data processor undertakes to carry out, on behalf of the Data controller, the processing of personal data as defined below.
Within the framework of their contractual relations, the Parties undertake to comply with the regulations in force applicable to the processing of personal data and, in particular, Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter, “GDPR”).

1.2 Qualification of the Parties. Qualification of the Parties. The Client is considered to be the “Data controller” and the Service provider is considered to be the Client's “Data processor” in accordance with the provisions of the General Data Protection Regulation (“GDPR”) of April 27, 2016.

1.3 Processing carried out by the Data processor. The Data processor is authorized to process, on behalf of the Data controller, the personal data necessary for the provision of a patient medical record containing the information required for the patient's care, and in particular, the verification of inclusion criteria in clinical trials in order to provide a therapeutic option for the patient.

The operations performed by the Data processor on the data are:

X Pseudonymization	X Preservation/archiving	☐Reconciliation or interconnection
☐ Collection	☐ Modification	☐ Limitation
X Reading	☐ Extraction	X Deletion or destruction
☐ Ranking	X Transmission	
X Registration	☐ Diffusion	

The purpose of the processing is: patient care, and in particular, verification of inclusion criteria in clinical trials to provide the patient with a treatment option.

The categories of data subjects concerned are:

- Healthcare professionals
- Patients monitored by these healthcare professionals

The personal data of the data subjects processed are:

- Healthcare professionals: personal identification data, professional data, contact details.
- Patients treated by these healthcare professionals: personal identification data, contact details, health data, genetic data, where applicable.

The personal data retention period for the Data processor is:

- two years in the active database as part of the service provision,
- then, after two years of inactivity of the healthcare professional account or the end of the contract, the data is pseudonymized and stored in an archive database for a period of two years (see Patient Information Sheet).

In any event, the Data processor shall retain the data processed during the provision of services for the duration of the agreement concluded between it and the Data controller. The Data processor is responsible for the necessary technical and organizational measures it implements to comply with the principle of minimizing the processing of personal data in the context of data retention.

1.4 Obligations of the Service provider as a Data processor. The Data processor undertakes to:

(i) process the data solely for the purpose(s) covered by the outsourcing agreement;

(ii) process the data in accordance with the documented instructions of the Data controller set out in the appendix to this agreement. If the Data processor considers that an instruction constitutes a breach of the European Data Protection Regulation or any other provision of Union or Member State law relating to data protection, it shall immediately inform the controller. Furthermore, if the Data processor is required to transfer data to a third country or to an international organization under Union law or the law of the Member State to which it is subject, it shall inform the controller of this legal obligation prior to processing, unless the relevant law prohibits such information on important grounds of public interest;

(iii) alert the Data controller of any instructions that do not comply with the law and regulations in writing to the following email address: [DPO email address of the Data controller]_____;

(iv) guarantee the confidentiality of personal data processed under this contract;

(v) ensure that persons authorized to process personal data under this contract:

- undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality;
- receive the necessary training in the protection of personal data

(vi) take into account, with regard to its tools, products, applications, or services, the principles of data protection by design and data protection by default.

1.5 Obligations of the Client as Data controller. The Data controller is required to fulfill its obligations under the GDPR, in particular with regard to the obligation to inform data subjects about processing operations at the time of collection of personal data, the maintenance of a record of processing activities, and more generally, compliance with the principles set out in the GDPR.

The Data controller further undertakes to:

(i) allow healthcare professionals to provide the processor with the personal data referred to in the processing specifications in connection with their use of Klineo;
(ii) document in writing any instructions concerning the processing of personal data by the processor;
(iii) ensure, in advance and throughout the duration of the processing, that the processor complies with the obligations set out in the European Data Protection Regulation;
(iv) supervise the processing, including conducting audits and inspections of the processor, if deemed necessary.

1.6 Exercise of individuals' rights. Where possible, the Processor shall assist the Controller in fulfilling its obligation to respond to requests from data subjects to exercise their rights: right of access, rectification, erasure, and objection; right to restriction of processing; right to data portability; right not to be subject to automated individual decision-making (including profiling). When data subjects submit requests to exercise their rights to the processor, the processor shall respond to them and inform the Data controller by email at the following address: [Email address of the Data controller's DPO]_____

1.7 Notification of personal data breaches. The Processor shall notify the Controller of any personal data breaches within a maximum of 72 (seventy-two) hours after becoming aware of them, by email to the following email address: [DPO email address of the Controller]_____. This notification shall be accompanied by any useful documentation to enable the Data controller, if necessary, to notify the competent supervisory authority of the breach.

This information must include at least the following:

- The nature of the data breach;
- The categories and volume of personal data concerned;
- The category and approximate number of individuals concerned;
- The existing and likely consequences of the breach;
- An estimate of the severity of the risk posed by the breach;
- The measures taken or planned to remedy, limit, or mitigate the breach;
- The name and contact details of the data protection officer, if one has been appointed, or, where applicable, the name and contact details of a contact person.

In the event of a data breach, in addition to the required measures, the Service provider shall take all reasonable and necessary measures to limit the consequences and prevent further leaks.

Furthermore, the Service provider shall provide the Customer, within the scope of the data concerned, with all necessary assistance to assess the extent and consequences of the data breach and to comply with the obligation to report data breaches and the duty to inform the persons concerned.

1.8 Assistance provided by the Data processor to the Data controller. The Data processor assists the Data controller, if necessary in view of the requirements of the supervisory authorities, in carrying out data protection impact assessments and prior consultation with the supervisory authority, as provided for by the GDPR.

1.9 Security measures. The processor undertakes to implement all technical and organizational security measures in the design of the product(s) supplied to the controller. In this regard, the Data processor undertakes to take into account the provisions relating to privacy by design provided for in Article 25 of the General Data Protection Regulation. Taking into account the state of knowledge, the costs of implementation, and the nature, scope, context, and purposes of the processing, as well as the risks, varying in probability and severity, that the processing presents to the rights and freedoms of natural persons, the Data processor shall implement appropriate technical and organizational measures in an effective manner and provide the necessary safeguards for the processing in order to meet the requirements of the GDPR and protect the rights of the data subjects.

At a minimum, the Data processor must ensure in particular that:

- Access to personal data for its staff members is configured and controlled;
- Policies for accessing incoming and outgoing data have been properly configured;
- A specific authentication procedure for accessing personal data is applied;
- Personal data is regularly backed up and that all backups are subject to strict security measures to ensure the availability, integrity, and confidentiality of the data;
- The security measures in place have been tested and are regularly tested as part of a quality control and information systems security process;
- Personal data is encrypted before being sent electronically and is transferred via a secure internet portal;
- Staff members are not able to access personal data remotely from their homes or via their own electronic devices, and no personal data is stored on such devices, with the exception of organized teleworking arrangements governed by an internal teleworking charter at the Data processor's premises that complies with the security requirements in the health sector, having informed the Data controller.

More generally, the Data processor undertakes to implement appropriate security measures, consisting in particular of:

- the means to ensure the ongoing confidentiality, integrity, availability, and resilience of the processing systems and services used;
- means to restore the availability of and access to Personal Data within an appropriate timeframe in the event of a physical or technical incident;
- a procedure to regularly test, analyze, and evaluate the effectiveness of technical and organizational measures to ensure the security of processing.

In addition, the processor provides a detailed list of the technical and organizational security measures implemented for the provision of services in Appendix A.

1.10 Disposal of data at the end of the contract. At the end of the Services relating to the processing of Personal Data, the processor undertakes to return all personal data to the Data controller or, where applicable, to the processor designated by the Data controller, without applying any additional charges. The Data controller undertakes to provide the Data processor with the information necessary to carry out the operation relating to the fate of the data.

In the event that the Client agrees to the storage of data by Klineo for the purpose of improving the algorithm and the patient journey for a specified period of time, Klineo will store the data of the individuals concerned in accordance with the established period (two years) in its capacity as an independent Data controller for this purpose.

1.11 Data processing register. In the event of sensitive data processing, the processor declares that it keeps a written register of all categories of processing activities carried out on behalf of the controller, including:

- the name and contact details of the controller on whose behalf it acts, any processors and, where applicable, the data protection officer;
- the categories of processing carried out on behalf of the Data controller;
- where applicable, transfers of Personal Data to a third country or to an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in Article 49, paragraph 1, second subparagraph of the GDPR, the documents attesting to the existence of appropriate safeguards;
- to the extent possible, a general description of the technical and organizational security measures.

1.12 Data Protection Officer. Each Party undertakes to appoint a Data Protection Officer in accordance with the provisions of Article 37 of the GDPR, if such appointment is mandatory for that Party.
Each Party declares that, on the date of signature of this Agreement, it has appointed the following as its Data Protection Officer:

	The Data controller	**The Data processor**
Email contact		dpo@klineo.fr

1.13 Documentation and audit. The Data processor shall provide the Data controller with the necessary documentation to demonstrate compliance with all its obligations and to enable audits, including inspections, to be carried out by the Data controller or another auditor appointed by it, and shall cooperate with such audits.

In the context of such audits, the Data controller or the auditor appointed by it shall not be authorized to access the Data processor's trade secrets, strategic information, or information that the Data processor has undertaken to keep confidential. The Data processor may object, in writing and with justification, to any control measure by the controller or the auditor appointed by him that would give them access to such data or information, without the controller being able to make any claim in this regard. Such refusal by the Data processor shall not impede the spirit of the GDPR and the overall objectives of the control carried out by the Data controller. The Data controller shall also ensure in all cases that the auditor and, more generally, the personnel carrying out the control are subject to appropriate confidentiality obligations and do not engage in any activity that competes with that of the Data processor.

1.14 Sub-processors. The Processor shall provide the Controller with the existing list of sub-processor prior to the signing of this Agreement.

The Data processor shall inform the Data controller of any planned changes in the addition or replacement of its Data processors, giving the Data controller the opportunity to object to such changes.

The Data processor remains fully liable to the Data controller for the performance, in whole or in part, of the obligations of its Data processors duly declared and accepted by the Client.

The Data processor declares the following sub-processor(s):

- OVH (HDS-certified Health Data Host)
- Brevo (emailing and CRM solution)

1.15 Transfer of data outside the European Union. The Data processor undertakes to use only means of processing personal data located within the territory of a member country of the European Economic Area and not to transfer personal data to a territory outside the European Economic Area, except in the following cases:

- The transfer is made to a country with an adequate level of personal data protection certified by the European Commission;
- The transfer is made to a company that has adhered to a specific mechanism recognized by the European Commission, or failing that, by the French data protection authority (CNIL);
- The transfer is covered by standard contractual clauses (SCCs) drawn up by the European Commission.

The Data processor undertakes to ensure that its affiliates and Data processors comply with these obligations.

The Data processor undertakes to inform the Data controller of the location of the premises where personal data of any kind is processed (hosting, backup, maintenance, administration, helpdesk).

1.16 Cooperation with the supervisory authority. Where necessary, the Parties undertake to cooperate jointly to respond to requests from the supervisory authority.

1.17 Data relating to persons acting on behalf of the Parties and collected in connection with the performance and management of the Contract

For the purposes of managing contractual relationships, the Parties are considered to be independent Data controllers and undertake to apply the regulations relating to the protection of personal data, in particular about informing the persons concerned.

Any person acting on behalf of the Data controller whose data is collected may exercise their rights of access, rectification, and opposition to the processing of their data by contacting the Data controller's Data Protection Officer.

Similarly, any person acting on behalf of the processor whose data is collected may exercise these same rights with the processor's Data Protection Officer.

Each Party undertakes not to retain the data of persons acting on behalf of the other Party beyond the term of the Contract, plus the legal limitation periods and any mandatory retention periods.

1.18 Right to compensation and liability

The Parties are liable for damages resulting from breaches of legal obligations on the one hand, and of their respective obligations described herein on the other.

The Data processor is fully liable to the Data controller for any direct or indirect damage relating to personal data resulting from any breach of its contractual obligations, as well as for the actions of its employees, agents, affiliates, or Data processors. It shall be required to compensate the Data controller for any such damage.

Furthermore, pursuant to Article 82 of the GDPR:

- The Data controller held liable for compensation for damage shall seek compensation from the Data processor for the portion of the compensation corresponding to its share of responsibility for the damage;
- The Data controller who has borne the entire cost of compensation for damage is entitled to claim from the Data processor the portion of the compensation corresponding to its share of responsibility for the damage.

In any event, the Data processor is required to provide, upon first request and at no cost, all necessary help and assistance to the Data controller in order to protect its rights.

Done in Paris, on [XX]

In two (2) original copies, one (1) for each Party.

_____	_____
The Data controller	The Data processor
Name	Name
Name and position to be indicated	Name and position to be indicated