Crossuite Data Processing Agreement

The Parties

The Client, hereinafter to be referred to as the PRACTICE,

and:

CROSSUITE bv, with its registered office at Uitbreidingstraat 390, 2600 Antwerp, Belgium
lawfully represented by Van den Putte, Joris and Debreuck, Nicolas, hereinafter to be referred to as *'CROSSUITE'*.

whereas:

A. The PRACTICE wishes to use a patient management platform in the form of a web application (hereinafter the 'Portal') that has been developed by Crossuite.
B. The PRACTICE and CROSSUITE have entered into an Agreement for that purpose.
C. Within the context of this Agreement CROSSUITE processes Personal Data that has been obtained by the PRACTICE
D. This Data Processing Agreement sets out the agreements reached between the PRACTICE and CROSSUITE on the processing of that Personal Data
E. In addition to that provided for in the Agreement, the Parties agree, in light of the GDPR and the Personal Data Protection Act, as follows.

Article 1. Definitions

1.1 In this Data Processing Agreement the following terms, always capitalised, have the following meanings:

a. Data Subject: The person to whom the Personal Data pertains, within the meaning of article 4(1) of the GDPR;
b. Processor: The Processor within the meaning of article 4(8) of the GDPR. In this Data Processing Agreement the Processor is CROSSUITE
c. Data Processing Agreement: This Data Processing Agreement, which is an inextricable part of the Agreement, for the purpose of setting down the agreements within the meaning of the GDPR
d. Agreement: All of the agreements/contracts concluded between the PRACTICE and CROSSUITE, including their annexes, for the purpose of using the Portal
e. Data Breach: The loss or unauthorised processing of Personal Data, or becoming aware of a shortcoming in the security that entails a considerable risk
f. Parties: the PRACTICE and CROSSUITE
g. Personal Data: Data that can be used to directly or indirectly identify a natural person, within the meaning of article 4(1) of the GDPR
h. Controller: The party within the meaning of article 4(7) of the GDPR; in this Data Processing Agreement the controller is the PRACTICE
i. Processing: Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, within the meaning of article 4(2) of the GDPR.

Article 2. Duration and termination

2.1 This Data Processing Agreement automatically comes into being once CROSSUITE's (licence) Agreement is signed.
2.2 This Data Processing Agreement ends by law at the time that the (licence) Agreement expires.
2.3 CROSSUITE shall, upon the termination of the Agreement, at the request of the PRACTICE and with the remuneration of reasonable costs, make the Personal Data available in a commonly used format to the PRACTICE or to a Third Party appointed by the PRACTICE.
2.4 CROSSUITE shall, after the transfer of the Personal Data to the PRACTICE, destroy any remaining Personal Data that could not reasonably be made available to the other Party. In that event, CROSSUITE shall also ensure that any Personal Data in the possession of Sub-Processors is likewise destroyed.

Article 3. Scope of the Data Processing Agreement and the Processing performed by CROSSUITE

3.1 CROSSUITE shall only process the Personal Data made available for the purpose of performing the Agreement.
3.2 The PRACTICE determines the purposes of the Processing of the Personal Data. CROSSUITE processes Personal Data on the instructions of the PRACTICE solely in order to facilitate the Portal.
3.3 The PRACTICE shall inform CROSSUITE of the purposes of the processing, insofar as such is not already contained in this Data Processing Agreement. Annexe 1 contains the processing purposes set out by the PRACTICE and it constitutes an inextricable part of this Data Processing Agreement. CROSSUITE shall not Process the Personal Data for a purpose other than those determined by the PRACTICE.
3.4 CROSSUITE shall only Process the Personal Data in the European Union.

Article 4. Security

4.1 CROSSUITE shall ensure that the Personal Data it Processes is adequately secured against misuse and unauthorised use.
4.2 CROSSUITE shall take suitable technical and organisational measures to secure the PRACTICE's Personal Data against loss or any form of unlawful processing.
CROSSUITE shall implement the required technical and organisational measures with respect to security in accordance with the NEN 7510 standard, for which CROSSUITE is certified (TPM 2017).
The data centres that CROSSUITE uses comply with the ISO27001 standard.
These measures are deemed to be at an adequate security level within the meaning of article 32 of the GDPR. The PRACTICE is entitled to, in consultation with CROSSUITE and while the Agreement is ongoing, have an independent expert assess compliance therewith, such as by means of performing an audit. The PRACTICE shall be responsible for all costs with respect to such an assessment.
4.3 CROSSUITE declares that the following measures have in any event been taken:

- Logical access control, 2-step authentication
- Physical measures for securing access
- SSL connections
- Registration of security incidents
- Purpose-bound access restrictions
- Checking awarded permissions

CROSSUITE can unilaterally amend these measures at any time, but only if such does not reduce the level of security.
4.4 The PRACTICE is responsible for compliance with the measures taken by the Parties (see CROSSUITE Agreement)
4.5 CROSSUITE is not responsible for the security being effective under all circumstances, although the security shall always comply with a level that is not unreasonable, taking into account the state of the art, the sensitivity of the Personal Data and costs associated with engaging that security.
4.6 At the request of CROSSUITE the PRACTICE shall, within 2 workdays, inform CROSSUITE in writing of the manner in which the PRACTICE is performing its obligations under the laws and legislation with respect to the protection of Personal Data, which in any event shall include the Personal Data Protection Act and the GDPR.
4.7 CROSSUITE shall support the PRACTICE in respect of the Processing in terms of the latter complying with its obligations under the GDPR. CROSSUITE shall assist the PRACTICE in respect of the Processing within the context of performing a data protection impact assessment in accordance with articles 35 and 36 of the GDPR.

Article 5. Audits

5.1 The PRACTICE has the right to periodically perform audits or have such performed in order to assess the agreements under this Data Processing Agreement.
5.2 CROSSUITE shall keep the supporting data required for the audits, such as system logs.
5.3 The persons that perform the audits shall adhere to the security procedures in effect at CROSSUITE.
5.4 CROSSUITE shall cooperate in the audit and provide all information reasonably relevant to the audit as soon as possible.
5.5 The audit costs are payable by the PRACTICE.
5.6 The PRACTICE shall not perform an audit earlier than 14 (fourteen) days after a written notification thereof. If the date and time of the audit are not convenient for CROSSUITE, it shall inform the PRACTICE thereof and propose an alternative date.

Article 6. Indemnifications

6.1 CROSSUITE indemnifies the PRACTICE from all legal actions by third parties, irrespective of their cause, with respect to the Personal Data or the performance of the Data Processing Agreement and/or Agreement, unless

CROSSUITE demonstrates that it acted in accordance with the PRACTICE's instructions and/or all technical and organisational measures for securing the Personal Data were taken, as set out in this Data Processing Agreement.

6.2 The PRACTICE indemnifies CROSSUITE from all legal actions by third parties, irrespective of their cause, with respect to the Personal Data or the performance of the Data Processing Agreement and/or Agreement, where it is determined that CROSSUITE acted solely in accordance with the PRACTICE's instructions.

6.3 If legal actions by third parties with respect to the Personal Data or the performance of the Data Processing Agreement and/or Agreement are due to a wilful act or gross negligence on the part of a party, then that party shall in any event indemnify the other party.

Article 7. Confidentiality

7.1 An obligation of confidentiality vis-à-vis third parties is in place for all Personal Data that CROSSUITE receives from the PRACTICE and/or collects or ought to collect for the purpose of Processing it under the Agreement.

7.2 CROSSUITE is aware the information that the client shares with CROSSUITE and stores in the Portal is confidential and company-sensitive. All CROSSUITE staff shall, for the duration of their employment and thereafter, as is stated in their employment contracts in a confidentiality clause, deal with the PRACTICE's information in a responsible manner.

7.3 CROSSUITE shall not use this information for a purpose other than that for which it received it, even where such information is converted into a form where neither the PRACTICE nor natural persons, such as the Data Subject, can be identified.

7.4 This obligation of confidentiality is not applicable insofar as the PRACTICE or the Data Subject have provided explicit consent for information to be provided to third parties.

7.5 If CROSSUITE uses the services of third parties, it shall unconditionally ensure that these third parties accept the same obligation of confidentiality as agreed to by the Parties and that they comply strictly with this obligation of confidentiality.

7.6 Staff with access to the PRACTICE's Personal Data:

1. CROSSUITE system administrators have full access to the PRACTICE's data for the purpose of:
   - installing a new version, build or update;
   - implementing patches and hotfixes;
   - creating a backup;
   - moving an environment.
2. Consultants, support staff and other CROSSUITE staff only have access to the data they have been permitted to access by the PRACTICE and only for that period for which they have received such permission from the PRACTICE.

Article 8. Reporting obligation

In the event of a Data Breach being discovered, CROSSUITE shall inform the PRACTICE as soon as possible and in any event within 24 hours of the discovery using 0032 2 888 91 79 or the following email address: info@crossuite.com. CROSSUITE shall under no circumstances inform the Data Subjects of the Data Breach, notwithstanding the obligation to remedy or limit the consequences of such breaches and incidents as soon as possible.

CROSSUITE shall furthermore, at the request of the Controller, make available all information that the PRACTICE deems necessary for the purpose of assessing the incident.

CROSSUITE undertakes, after the discovery of a Data Breach, to keep the PRACTICE informed of the measures taken in order to limit the extent of the Data Breach or prevent such from occurring in the future.

CROSSUITE has a solid action plan on how to deal with and settle Data Breaches and shall provide the PRACTICE with access thereto, at the latter's request. The Processor shall inform the Controller of any material changes to that action plan.

CROSSUITE shall leave it to the PRACTICE to make reports to the supervisory authority or authorities.

CROSSUITE shall cooperate in full with, where necessary and in the shortest possible space of time, providing supplementary information to the supervisory authority or authorities and/or Data Subject or Subjects. In that respect, CROSSUITE shall in any event provide that information set out in annexe 3 to the Controller.

The Processor keeps a detailed logbook updated of all (suspected and actual) Data Breaches, as well as the measures taken as a result of such Data Breaches in which at least that information referred to in annexe 3 is recorded, and shall provide access thereto to the PRACTICE at the latter's request.

Article 9. Rights of the Data Subject

If the PRACTICE receives an application from a Data Subject whose Personal Data is processed to exercise their rights pursuant to the GDPR, such as the right to object to the Processing of their Personal Data or the right to its deletion, the PRACTICE shall forthwith inform CROSSUITE thereof.

CROSSUITE undertakes to forthwith, and no later than within 7 days of receipt of such an application, perform the instruction received from the PRACTICE and either provide the requested information or implement the requested change to the Personal Data, or delete and destroy that Personal Data.

Article 10. Engaging third parties

10.1 The PRACTICE grants general permission to CROSSUITE to appoint sub-processors for the purpose of performing the processing activities that are the subject of this Data Processing Agreement.

10.2 If CROSSUITE wishes to engage a sub-processor within the meaning of this article, CROSSUITE undertakes to conclude a written agreement with that sub-processor that at least comprises the guarantees and obligations arising from this Agreement.

10.3 CROSSUITE shall keep an updated register of the third parties and sub-processors it has engaged, in which the identity, location and a description of the activities performed by the third parties or sub-processors are recorded, as well as any further conditions imposed by the PRACTICE. This register shall be appended to this Data Processing Agreement as annexe 4 and shall be kept updated by CROSSUITE. Where CROSSUITE intends to change sub-processors, it shall inform the PRACTICE thereof in advance, and the PRACTICE can object thereto in writing, providing motivations for such, within five workdays. Where a written objection is not received within the aforementioned period, the PRACTICE is deemed to have consented to the change.

Article 11. Liability

11.1 CROSSUITE is solely liable for the Processing of Personal Data through the service it offers under the Agreement, subject to the conditions set down in the Data Processing Agreement. CROSSUITE is explicitly not liable for all other Processing of Personal Data, which in any event includes but is not limited to the collection of the Personal Data by the PRACTICE and/or third parties.

11.2 Responsibility for the purposes and the lawfulness of the processing of the Personal Data that is Processed using a service provided by CROSSUITE lies wholly with the PRACTICE.

11.3 If the PRACTICE demands compensation from CROSSUITE on the grounds of noncompliance with this Data Processing Agreement or the applicable legislation, then the total liability on the part of CROSSUITE shall be limited to the total of the invoiced services for the previous calendar year, unless the sum for which the company and/or professional liability of CROSSUITE is insured is lower (up to 1250,000 euros). For the application of this article, a series of associated incidents are deemed to be a single event.

11.4 CROSSUITE is not liable for any form of indirect damage, such as but not limited to busines interruption, reduced goodwill, lost savings, lost profits, damage to reputation or any other form of indirect, incidental or consequential loss, irrespective of the nature of the action.

11.5 For the duration of the Data Processing Agreement the parties shall be adequately insured and shall maintain such insurance. The insurance terms and conditions can be viewed upon request.

Article 12. Disputes resolution

12.1 The law of the nation in which CROSSUITE is established is solely applicable to the Data Processing Agreement.

12.2 All disputes that arise as a result of this Data Processing Agreement are to be resolved in the same manner as set out in the Agreement.

Article 13. Order of priority

The Agreement is applicable to the Data Processing Agreement. Where there is a conflict between the (licence) Agreement and the Data Processing Agreement, that provided for in the Data Processing Agreement takes priority.

ANNEXE 1

A. Categories of Data Subjects

The persons to which the Personal Data pertains are in any event:

- patients
- lessees

B. Type of Personal Data

The Personal Data processed by the PROCESSOR/CROSSUITE is in any event:

- Name and address, telephone numbers, email address(es)
- Healthcare insurer
- Social security identification number
- Description of pathology
- Date of birth
- Name of GP
- Profession
- Hobbies and sports
- Family makeup

C. Nature and purpose of the processing

The nature of the processing: for the purpose of treating persons, their examination and treatment records are documented.

The Personal Data is in any event processed for the following purposes:

Purposes of the processing:

- Processing so that adequate treatment can be provided, and monitoring and evaluating it;
- Processing so that the patient and/or GP can be reached;
- Processing so that an appointment can be made for the patient to be treated;
- Processing so that the treatment(s) can be charted;
- Processing so that the costs of the treatment(s) can be charged to the healthcare insurer;
- Processing so that, with the consent of the patient, a report can be sent to third parties.

Annexe 2: Overview of the security measures

Information security and privacy policy

Our information security and privacy policy complies with the GDPR and any guidelines issued by the authorities, and it is in line with the ISO 27001 and NEN 7510 standards for information security. This policy is communicated internally and implemented in concrete terms by means of documented procedures.

Certification

An information security management system (ISMS) is in place, which was created and instituted in accordance with the ISO 27001 and NEN 7510 standards for information security. The system has been certified by an independent auditor, Dekra.

Staff

Staff are informed of their responsibilities with respect to privacy and information security and we monitor their fulfilment of those responsibilities. Staff that have access to client/patient data are bound by confidentiality.

Contract management for (Sub-)Processors

A data processing agreement is concluded with every permitted (Sub-)Processor, which contractually obliges the (Sub-)Processor to comply with the same obligations for the Processing as contained in the data processing agreement.

Security incidents & response

A documented security incident response plan is in place that is capable of detecting, remedying and reporting data breaches, in accordance with the obligations contained in the data processing agreement.

Encryption of data in transit

All the online traffic to Crossuite runs via an SSL-encrypted connection (Secure Socket Layer, or the secure transmission of information and protection of personal data), and we only accept traffic through port 443.

When you first visit our website, Crossuite sends a Strict Transport Security Header (HSTS) to your browser, which means your connection will henceforth be secured via HTTPS, the safest internet protocol – even if you click onto our website using an unencrypted link, which specifically starts with ‘http://’.

Patch management/Network and system security

We periodically assess whether there are vulnerabilities within the applications, systems and networks we use. Patches and updates for discovered vulnerabilities are installed.

Crossuite uses Amazon Web Services (AWS) for storing data. These servers are subjected to periodic evaluations so that they comply with the latest standards. Because we use AWS as our data centre, our infrastructure is accredited for:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (now SAS 70 Type II)
- PCI Level 1
- C5 Operational Security

- ENS High
- IT-Grundschutz

Further information on the security of AWS is available through this link.

Password policy and storage

In order to create a Crossuite account you must choose a password containing at least 6 characters. We do not store user passwords in text format and only use non-decipherable password hashes that have been encrypted using Bcrypt (including per-user-random-salt). This means we protect users from rainbow table attacks and attempts to decipher the encryption syntax.

If a user inputs an incorrect password multiple times (more than five times), the account is locked in order to prevent brute-force attacks (a method for cracking passwords using many attempts). The user can then only log-in again by requesting a new password.

In order to further secure your account we also use Two-Factor Authentication (an additional layer of protection that is only available to the user) by means of email, Google Authenticator or SMS.

Our team uses strong and unique passwords for Crossuite accounts and uses Two-Factor Authentication for every device and service. We also encourage all our staff to use password managers such as LastPass for generating strong passwords and storing them in a safe location.

We also encrypt the local hard drives and screen savers are automatically triggered.

Access management

Our application's admin functions can only be accessed by a select group.
User access is revoked or changed in good time in the event of any changes to the status of staff, suppliers, clients, business partners or third parties.

Physical access control

Suitable measures are in place (such as locks and alarm systems) to secure the rooms where Personal Data is Processed against unauthorised access.

Logging

Logging is used to see which users are logged in and when, in order to check what processing of Personal Data is performed by which user.

Application development – security principles

In order to comply with all safety standards, we employ strict code reviews for every change or addition to our application.

Vulnerability disclosure
Ever since Crossuite was launched we have actively encouraged users to quickly report any issues in our application and help us to guarantee the safety and reliability of our platform. We deal with and respond to all notifications as quickly as possible.

Annexe 3: Overview of the information to be provided in the event of an incident

CROSSUITE shall in any event provide the following information to the PRACTICE in the event of an incident that concerns the Controller's Personal Data:

- the (suspected) cause of the breach;
- the (known and/or anticipated) consequences;
- the (proposed) solution;
- contact details for following up on the notification;
- the number of persons whose Personal Data was affected by the breach (if the exact number is not known, the minimum and maximum number of people whose Personal Data was affected by the breach);
- a description of the group of persons whose Personal Data was affected by the breach;
- the type or types of Personal Data affected by the breach;
- the date upon which the breach occurred (if the exact date is not known, the period within which the breach occurred);
- the date and time when the breach became known to the Processor or to the third party or sub-processors engaged by the Processor;
- whether or not the data was encrypted, hashed or rendered incomprehensible or inaccessible to third parties in another manner;
- what measures have already been taken to remedy the breach or limit the consequences thereof.

Annexe 4: Overview of the sub-processors

Sub-processor 1:	Bart.SK SRO
Description of the activities	Resource partner

Sub-processor 2:	LINK Mobility Sp. z o.o.
Description of the activities	Sending SMSs

Sub-processor 3:	AWS Europe
Description of the activities	Hosting partner

Sub-processor 4:	Stripe
Description of the activities	Payment processing