Data Processing Agreement (DPA)

Synkro Clinic and Synkro Motion

Synkro · Thomas Theben Leutenez, self-employed

Version 3.9 · November 2026

Between the parties

This Data Processing Agreement (hereinafter the “DPA”) is concluded, in accordance with Article 28 of Regulation (EU) 2016/679 (hereinafter the “GDPR”), between:

The Controller: the Professional, whether Healthcare Professional or Sports Professional, identified by the information provided at registration, who uses Synkro Clinic or Synkro Motion in the course of their professional activity, whether they are a Licence Holder, in a trial period or in paused access, as well as the sports entity that is the controller under the conditions of Article 14.5 (hereinafter the “Controller”);

The Processor: Synkro, identified as follows (hereinafter “Synkro”):

Publisher	Thomas Theben Leutenez, self-employed sole trader under Belgian law, trading under the name Synkro (“Synkro”)
Registered office	11 Clos Joseph Otten, 1090 Jette (Belgium)
Enterprise number (CBE)	1037.237.034
VAT status	Taxable person under the special VAT exemption scheme for small businesses (Article 56bis of the Belgian VAT Code)
Contact	contact@synkroclinic.com, +32 497 32 27 80
Data protection contact point	dpo@synkroclinic.com
Hosting	Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855 Luxembourg; data hosted in the AWS Paris region (eu-west-3), in France

The Controller and Synkro are hereinafter referred to together as the “Parties”.

Preamble

Synkro publishes Synkro Clinic and Synkro Motion, two applications intended for professionals who monitor persons in the context of care or sports coaching. Their use involves the processing, on behalf of the Controller, of personal data relating to the persons they monitor, including data concerning health.

This DPA governs that processing. **It applies to every Professional and every entity, in the healthcare sector and in the sports sector alike.** It consists of a common core, applicable to every Controller, and of provisions specific to each profile, set out in Article 13 (“Provisions specific to healthcare professionals (Synkro Clinic)”) and Article 14 (“Provisions specific to sports professionals

(Synkro Motion)"). In the event of conflict, the provisions specific to the profile prevail over the common core.

The applicable profile depends on the profile of the Controller, and not on the product used, according to the rule set by the Terms of Use, Article 3: a Healthcare Professional falls under Article 13 for the entirety of their use, including biomechanical analysis and the monitoring of athletes outside a care setting, whose data is processed as data concerning health covered by professional secrecy; any other professional falls under Article 14.

The DPA forms an integral part of the contractual framework formed by Synkro's Terms of Use, Terms and Conditions of Sale and Privacy Policy. Each Professional accepts it personally when creating their account; a Licence Holder who has not yet accepted it accepts it no later than when activating their Licence or at their first login.

1. Definitions

The terms used in this DPA have the meaning given to them by the GDPR. In addition, the following terms, when capitalised, have the meaning given below, in both the singular and the plural. These definitions are common to the Terms of Use, the Terms and Conditions of Sale, the Privacy Policy and the DPA.

- **"Application"**: Synkro Clinic or Synkro Motion, as the case may be, accessible via web browser and via mobile application.
- **"Professional"**: any person who uses the Application in the course of their professional activity to monitor Monitored Individuals, whether they are a Licence Holder, in a trial period or in paused access. A Professional is either a Healthcare Professional or a Sports Professional.
- **"Healthcare Professional"**: any person registered with a professional order or holding a visa or an authorisation to practise a healthcare profession.
- **"Sports Professional"**: any other Professional, in particular a physical trainer, a coach, a bike fitter who does not practise a healthcare profession, or a sports entity.
- **"Monitored Individual"**: the person whom a Professional monitors by means of the Application. They are referred to as the **"Patient"** when the monitoring falls under a Healthcare Professional and as the **"Athlete"** when it falls under a Sports Professional.
- **"Record"**: all the information that a Professional holds on a Monitored Individual in the Application (assessments, notes, measurements, questionnaires, tests, exercises, videos, analyses, documents, appointments and, where applicable, Administrative Module data).
- **"Subscription"**: the paid subscription contract concluded with Synkro under the Terms and Conditions of Sale, on a monthly or annual basis, which carries one or more Licences.
- **"Subscriber"**: the natural or legal person who concludes the Subscription and pays its price (practitioner, practice operated through a company, club, federation or other entity).
- **"Licence"**: the personal right to use the Application under an offer, assigned to a single natural person.
- **"Licence Holder"**: the natural person to whom a Licence is assigned through the activation of a Licence Code. The Subscriber may themselves be a Licence Holder.

- **“Licence Code”**: the single-use code, in the format SYNK-XXXX-XXXX, which allows a Licence to be assigned to its Licence Holder.
- **“Practice”** and **“Team”**: the grouping of Professionals within the Application for the purpose of working together, called a “practice” in Synkro Clinic and an “organisation” or “group” in Synkro Motion (hereinafter “Team”). The rules for sharing Records within a Practice or a Team are set out in Article 11 of the Terms of Use.
- **“Administrative Module”**: the billing functions of Synkro Clinic and its services connected to the eHealth platform and to MyCareNet, described in Article 14.8 of the Terms of Use.
- **“Biomechanical Analysis”**: the automated video movement analysis feature, in two or three dimensions, described in Article 9 of the Terms of Use.

2. Purpose and duration

2.1. Purpose

The DPA defines the conditions under which Synkro processes, as processor, the personal data contained in the Controller’s Records, as well as the respective obligations of the Parties.

The DPA does not cover the processing for which Synkro is itself the controller: account management, invoicing and payment, security of the service and technical logs, fraud prevention, user relations and usage statistics. This processing is described in the Privacy Policy.

2.2. Duration

The DPA takes effect upon the creation of the Professional’s account or upon the activation of their Licence, whichever occurs first. It remains in force as long as Synkro holds data on behalf of the Controller, including while their access is paused. The confidentiality obligations survive its termination.

3. Licences, subscription and capacity of controller

3.1. Each Licence Holder is the controller of their own Records

Each Licence Holder is the controller of the Records they create or hold in the Application. Paying for a Licence confers on the Subscriber no capacity and no right over the Records of the Holder of that Licence: the Subscriber has no access to any Record merely because they pay for the Licence. Synkro receives instructions relating to a Record only from the Controller responsible for it, through that Controller’s own account.

A Licence Holder who works on behalf of an employer or an entity and accepts this DPA in that context declares that they are authorised to do so. The allocation of responsibilities between them is a matter for their relationship, to which Synkro is not a party.

3.2. Sharing within a Practice or a Team

Another Professional’s access to a Record never results from invoicing. It results solely from membership of a Practice or a Team, which each Professional chooses to join, according to the rules of the Terms of Use, Article 11:

- **in Synkro Clinic**, each Record is private by default. Sharing a Record with the Practice constitutes an instruction; the members access it according to the right granted to them by the Practice administrator (“view” or “view and edit”). Where the Practice administrator has chosen to have new Records shared from their creation, the Controller who remains a member of the Practice gives that instruction for their new Records and may withdraw the sharing at any time. The Practice’s administrative accounts have access only to the administrative data of the Patients (identity, contact details, health insurance fund) and to the calendars, never to health data or to invoicing;
- **in Synkro Motion**, each Record has a scope chosen by the Controller (private, group or organisation), private by default; each choice of scope constitutes an instruction.

A Controller who shares their Records:

- ensures that they have a legal basis for such sharing;
- informs the Monitored Individuals in advance and obtains their agreement where applicable law or the nature of the data so requires;
- limits the sharing to what is necessary and ends it when it is no longer justified, where applicable by withdrawing the sharing of the Record, by leaving the Practice or by changing the scope of the Record.

A member who accesses a shared Record is liable for the use they make of it. Synkro provides the technical means of sharing, logs access and never decides its extent. The departure of a member from the Practice or the Team ends their access to the other members’ Records; it has no effect on the Records for which that member is themselves responsible, which they retain.

3.3. End of the Licence or of the Subscription

When the Subscription ends (termination, non-payment), the Licence Holder’s access is paused at the end of the paid period. When the Subscriber releases the Licence, or the Licence Holder leaves it, access is paused immediately; the Subscriber notifies the Licence Holder in advance (Terms and Conditions of Sale, section “Licences”). Access is also paused at the end of the Free Trial when no Subscription has been concluded and no Licence Code activated.

During the pause, the Records are retained and remain exportable for at least ninety days, and are then retained as long as the account exists, under the conditions of the Privacy Policy, section “Retention periods”. The Licence Holder may at any time take out their own Subscription or activate a new Licence Code and regain access to their Records without loss.

4. Description of the processing

4.1. Nature of the operations

Hosting, recording, organisation, storage, consultation, automated calculations (scores, indicators), automated video analysis, assisted structuring of texts, presentation, sharing on instruction, disclosure to the recipients designated by the Controller, export and erasure.

4.2. Purposes

Synkro processes the data solely for the purpose of providing the Controller with the features of the Application that they use to monitor the Monitored Individuals, of ensuring their security and traceability, and of carrying out the Controller's instructions. The purposes specific to each profile are set out in Articles 13 and 14.

4.3. Categories of data subjects

The Monitored Individuals and, for the data concerning them in a Record, the members of the Practice or the Team and the third parties whose identity appears in it. The categories specific to each profile are set out in Articles 13 and 14.

4.4. Categories of data

The categories of data specific to each profile are set out in Articles 13 and 14. The following are common to both profiles:

- the identification and contact data of the Monitored Individual, as well as their account credentials when they use the Application;
- the videos and images uploaded to the Application, and the results of their automated analysis (joint angles, ranges of motion, symmetry, movement indicators);
- the monitoring data entered by the Controller or by the Monitored Individual;
- the log of access to Records.

Videos and three-dimensional reconstructions are processed solely for the purpose of producing movement indicators. They are not subject to any biometric processing for the purpose of uniquely identifying a natural person within the meaning of Article 9(1) of the GDPR.

4.5. Artificial intelligence assistance

In Synkro Clinic, at the request of the Controller, a language model run by the Amazon Bedrock service sorts a free text, typed or dictated, into the fields of a session note and pre-fills fields of the Record. The data transmitted may include the identity and contact details of the Monitored Individual. The Amazon Bedrock service is not used for the Biomechanical Analysis.

This processing is carried out by means of an inference profile restricted to the European Union, which may route requests to several AWS regions of the European Union. In accordance with the AWS service terms, the content submitted to this service is neither retained by it nor used to train models.

The proposals generated are presented to the Controller, who reviews, modifies or discards them, and remains solely responsible for the content of the Record. No proposal is sent directly to the Monitored Individual. This is not an automated individual decision within the meaning of Article 22 of the GDPR.

Synkro keeps a log of these calls, which contains usage metrics and identifiers but not the content of the texts submitted or of the responses obtained, and retains it for twelve months. The details are set out in the Privacy Policy, section “Artificial intelligence assistance”.

4.6. Duration of the processing

The data is processed throughout the life of the Controller's account, including while their access is paused, and until its deletion under the conditions of Article 7.8. The applicable retention periods are set out in the Privacy Policy, section "Retention periods".

5. Obligations of the Controller

The Controller undertakes to:

- have a valid legal basis for each processing operation entrusted to Synkro, under the conditions specified for their profile in Articles 13 and 14;
- inform the Monitored Individuals of the processing of their data, in particular by telling them that they use the Application and by referring them to Synkro's Privacy Policy;
- obtain the consents required for their profile and, for minors, apply the rule of Article 6;
- record in the Application only persons whom they actually monitor, and upload to it only the data necessary for that monitoring;
- assess, before joining a Practice or a Team or changing the scope of a Record, the resulting access for the other members (Article 3.2);
- keep their own record of processing activities and take the security measures incumbent upon them, in particular the protection of their credentials and devices;
- handle the requests to exercise rights sent to them by the Monitored Individuals;
- export their Records before any deletion provided for in Article 7.8 where they are required to retain them for longer;
- give Synkro lawful and documented instructions.

5.1. Video recording

The Controller is responsible for the conditions in which videos are made. They inform the person being filmed, obtain their prior agreement, upload videos showing identifiable third parties only with their agreement and comply with the rules applicable at the place of recording.

6. Minors

The following rule applies to any Monitored Individual who is a minor, whether Patient or Athlete, regardless of the country:

- **under thirteen years of age**: the account is created and any consent is given exclusively by the holder of parental authority;
- **from thirteen to eighteen years of age**: consent is given jointly by the minor and by the holder of parental authority.

This rule is more protective than the thresholds laid down by national laws (thirteen years in Belgium, fifteen years in France); it therefore applies in all cases. The Professional verifies the age of the Monitored Individual and obtains the required consents before sending them an invitation code and before any video recording.

Synkro technically makes the creation of a Monitored Individual's account conditional on the entry of an invitation code provided by the Controller. The exercise of the rights of a Monitored Individual who is a minor is set out in the Privacy Policy, section "Minors".

7. Obligations of Synkro

7.1. Documented instructions

Synkro processes the data exclusively on the documented instructions of the Controller. These instructions consist of: this DPA, the Terms of Use, the features of the Application as used by the Controller, the settings of their account and the actions they trigger (in particular joining a Practice or a Team, choosing the scope of a Record, enabling synchronisation with a Google calendar, a submission to a health insurance fund, an export or a deletion). The same applies to transfers to a third country.

If Synkro is required to carry out processing under Union law or Belgian law, it informs the Controller before the processing, unless that law prohibits it on important grounds of public interest. Synkro immediately informs the Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

Synkro does not use the data of the Records for its own purposes, subject only to Article 8.

7.2. Confidentiality

Synkro ensures that the persons authorised to process the data are subject to a contractual obligation of confidentiality, are informed of the requirements of the GDPR and of the specific features of data concerning health, and access the Records only where necessary (support requested by the Controller, security, incident), within the limits of that necessity and with traceability.

7.3. Security of processing

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 to the rights and freedoms of individuals, Synkro implements the appropriate technical and organisational measures within the meaning of Article 32 of the GDPR, in particular:

- hosting with Amazon Web Services, Paris region (eu-west-3), data stored in France;
- encryption at rest: AES-256 by means of AWS KMS for the database, and AES-256 for the storage of files and videos, supplemented by specific encryption of certain sensitive fields, including the NISS (national registration number);
- encryption in transit (HTTPS, TLS 1.2 minimum);
- hashed passwords (bcrypt) and time-limited session tokens;
- partitioning of access: each Professional has access only to the Records they hold and to those to which the sharing rules of their Practice or Team give them access (Article 3.2); in Synkro Clinic, access checked by the server according to the user's profile (Professional or administrative account) and their right ("view" or "view and edit"), denied by default; confidential information visible only to its author and encrypted;
- logging of access to Records; application logs stripped of data concerning health at source;

- Professionals' eHealth certificates encrypted (AES-256-GCM), password never stored, sessions limited to twelve hours, each upload, session opening and signed submission logged and visible to the Professional, withdrawal possible at any time;
- storage of the other technical secrets in an encrypted vault (AWS Secrets Manager);
- principle of least privilege for access to the infrastructure, reserved for Synkro's authorised persons, and periodic review of such access;
- automatic backups of the database and of files, under the conditions of the Privacy Policy, section "Retention periods";
- infrastructure monitoring with alarms.

Synkro may change these measures, provided that it does not reduce the overall level of security.

7.4. Sub-processors

The Controller gives Synkro a general authorisation to use sub-processors. At the date of this DPA, the sub-processors are those indicated as such in the table below, which is identical to the one in the Privacy Policy; the other providers and recipients are listed for information and do not process Record data on behalf of the Controller, with the exception of Google Calendar, a recipient that the Controller personally chooses to enable.

Provider	Role	Data concerned	Location and safeguards	Capacity
Amazon Web Services EMEA SARL (Luxembourg)	Hosting of the application and the data (computing, database, storage, backups, secrets, logs), computation of the Biomechanical Analysis, artificial intelligence assistance (Amazon Bedrock)	All data	AWS Paris region (eu-west-3). Amazon Bedrock: inference profile restricted to the European Union, which may route requests to several AWS regions of the European Union	Sub-processor
Resend	Sending of transactional e-mails (registration, security, invitations, appointment confirmations and reminders, information on the trial and the Subscription)	Recipient's e-mail address and name, content of the message	United States; EU-US Data Privacy Framework and/or standard contractual clauses of the European Commission	Sub-processor

Provider	Role	Data concerned	Location and safeguards	Capacity
Expo (650 Industries, Inc.)	Routing of mobile application notifications, then relayed by Apple or Google	Technical identifier of the device, title and text of the notification, which may include the name of a Monitored Individual and the time of an appointment	United States; standard contractual clauses of the European Commission or EU-US Data Privacy Framework	Sub-processor
Stripe (Stripe Payments Europe Limited, Ireland)	Payment and management of Subscriptions	Identity and contact details of the Subscriber, payment data; no Record data	European Union; transfers to the United States governed by the EU-US Data Privacy Framework and/or the standard contractual clauses of the European Commission	Provider of Synkro for its own processing; no Record data
Google (Google Calendar)	Two-way synchronisation with the Professional's Google calendar, only if they enable it	Appointments entered in the Google calendar, with the name of the Monitored Individual and the appointment note	According to the contract between the Professional and Google	Independent recipient, chosen by the Professional
Google (Google Fonts)	Loading of the applications' fonts	IP address and technical information about the browser or device; no account or Record data	United States; standard contractual clauses of the European Commission or EU-US Data Privacy Framework	Independent recipient
Calendly (Calendly LLC)	Appointment booking module integrated into Synkro's websites	Name, e-mail address and information entered in the module; IP address	United States; standard contractual clauses of the European Commission or EU-US Data Privacy Framework	Provider of Synkro for its own processing; no Record data
Vercel (Vercel Inc.)	Hosting of Synkro's public websites	IP address and pages requested by visitors	United States; standard contractual clauses of the European Commission or EU-US Data Privacy Framework	Provider of Synkro for its own processing; no Record data

Provider	Role	Data concerned	Location and safeguards	Capacity
OpenStreetMap / Nominatim (OpenStreetMap Foundation, United Kingdom)	Display of maps and address search in the directory of practitioners	IP address; practice address of the Professionals and addresses searched	United Kingdom, which benefits from an adequacy decision of the European Commission	Independent recipient

Amazon Web Services holds, in particular, ISO 27001 and SOC 2 certifications, as well as Health Data Hosting (HDS) certification for infrastructure hosting; its data processing agreement is incorporated into its service terms.

Synkro imposes on each sub-processor, by contract, data protection obligations at least equivalent to those of this DPA, in particular sufficient guarantees to implement appropriate technical and organisational measures. Synkro remains fully liable to the Controller for the performance of their obligations by its sub-processors.

Synkro informs the Controller, by e-mail and in the Application, of any addition or replacement of a sub-processor at least thirty days before it takes effect. The Controller may object in writing, on legitimate grounds relating to data protection, during this period. The Parties then seek a solution in good faith. Failing this, the Controller may stop using the service and, if they are also a Subscriber, terminate their Subscription free of charge with effect from the date on which the change takes effect; in all cases, they retain the right to export their Records provided for in Article 7.8.

Nor are the recipients to whom the Controller decides to disclose data, in particular the health insurance funds and the platforms referred to in Article 13.4, sub-processors of Synkro.

7.5. Assistance with the exercise of rights

Synkro assists the Controller, by appropriate technical and organisational measures and insofar as possible, in responding to requests to exercise the rights of Monitored Individuals (access, rectification, erasure, restriction, portability, objection, withdrawal of consent). The Application allows the Controller to consult, correct, export and delete the Records. When a Monitored Individual contacts Synkro directly about a Record, Synkro forwards the request to the Controller within five working days, does not respond to the Monitored Individual on the merits without the Controller's instruction, and provides the Controller with the necessary technical assistance.

The deletion by a Monitored Individual of their account in the Application ends their access. It does not entail the deletion of the Record held by the Controller: the Record is detached from the deleted account and remains intact with the Controller, who is responsible for deciding on any erasure request, in compliance with their own retention obligations.

7.6. Assistance with security, impact assessment and prior consultation

Synkro assists the Controller in ensuring compliance with the obligations laid down in Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to it. In particular, it provides the Controller, on request, with a description of the processing operations and security measures useful for carrying out their data protection impact assessment and, where applicable, the prior consultation of the supervisory authority.

7.7. Notification of data breaches

Synkro notifies the Controller of any personal data breach affecting their Records without undue delay after becoming aware of it, and at the latest within forty-eight hours. The notification describes, insofar as this information is available, the nature of the breach, the categories and approximate number of persons and records concerned, its likely consequences and the measures taken or proposed to remedy it and mitigate its effects. Information that is not immediately available is communicated as soon as it becomes available.

It is up to the Controller to notify the breach to the supervisory authority and, where applicable, to communicate it to the data subjects; Synkro assists them in doing so. Synkro's internal breach management procedure is available on request.

7.8. Export, return and deletion of data

Export. The Controller may export their Records from the Application under the conditions of the Terms of Use, section "Data export and portability": in structured formats (JSON, CSV or ZIP archive, depending on the product), throughout the duration of their access and throughout any pause of that access, and in any event for at least ninety days after the end of their Subscription, their Licence or their trial. This export constitutes the return of the data within the meaning of Article 28(3)(g) of the GDPR.

Deletion. Synkro deletes the Controller's Records when their account is deleted, at their request or for inactivity under the conditions of the Privacy Policy, section "Retention periods" (in Synkro Clinic, never for inactivity when the account holds Records). Access is deactivated as soon as the request is made; the deletion can be cancelled for thirty days using the link received by e-mail; at the end of this period, **the account and all the Records for which the Controller is responsible are permanently deleted**. The accounts of the Monitored Individuals are not deleted, but no longer give access to these Records. The Controller exports their Records before requesting deletion.

Deleted data disappears from the backups no later than thirty days after its deletion. Synkro retains no copy of the Records, except where it is subject to a legal obligation of its own.

The deletion of the account of a member of a Practice or a Team ends their access to the other members' Records, without affecting those Records, which remain with the Controller responsible for them. In Synkro Clinic, what that member has recorded in them remains in those Records, under their name, together with the record of their access.

7.9. Documentation and audits

Synkro makes available to the Controller, on request, the information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR: record of processing activities kept as processor, list of sub-processors, description of the security measures, breach management procedure and certification attestations of its sub-processors.

Synkro allows audits, including inspections, to be carried out by the Controller or by an auditor mandated by the Controller and bound by confidentiality. Except in the event of a data breach or a request from a supervisory authority, the audit is announced at least thirty days in advance, covers only the processing carried out on behalf of the Controller, takes place at most once a year, during business hours, and may not undermine either the security of the service or the confidentiality of other users'

data. Synkro may offer to respond first by means of documents and written statements. The costs of the audit are borne by the Controller, unless the audit reveals a significant breach by Synkro of its obligations.

8. Operating statistics and research

Synkro produces aggregated operating statistics (for example the number of Records, analyses or uses of a function), which contain no content from the Records or any personal identifier and do not allow a person to be traced. These statistics are anonymous data that no longer fall within the scope of the GDPR (Recital 26).

No Record data is currently used for research purposes or to improve algorithms. An optional consent to research is obtained from Patients in the Application; should Synkro one day use data for these purposes, only anonymised data would be used, and the Privacy Policy and this DPA would be updated beforehand, under the conditions of Article 11.

No video is used to improve the algorithms.

9. Transfers outside the European Union

The Records are hosted in France (AWS, Paris region, eu-west-3). Artificial intelligence processing is carried out in the European Union, by means of an inference profile restricted to the European Union which may route requests to several AWS regions of the European Union.

Certain items from a Record may be transferred to the United States by sub-processors: the e-mail address and name of a Monitored Individual in an e-mail routed by Resend, their name and the time of an appointment in a notification routed by Expo. These transfers are governed as indicated in Article 7.4. When the Controller enables synchronisation with a Google calendar, the appointments entered in that calendar are processed by Google in accordance with the contract between them. The transfers carried out by Stripe concern exclusively the Subscriber's billing data.

Any new transfer of Record data outside the European Union would be subject to the procedure of Article 7.4 and to the existence of appropriate safeguards within the meaning of Chapter V of the GDPR.

10. Liability

Each Party is liable for damage caused by processing that does not comply with the GDPR, under the conditions of Article 82 of the GDPR. Synkro is liable for the failures of its sub-processors, in particular the hosting provider, as for its own; only force majeure, within the meaning of the Terms and Conditions of Sale, section "Force majeure", releases it from liability.

In relations between the Parties, Synkro's liability is subject to the cap provided for by the Terms and Conditions of Sale, section "Liability", except in the case of gross negligence or wilful misconduct. This cap does not limit the rights that data subjects derive from the GDPR.

11. Interrelation, amendments and end

- **Interrelation**: in the event of conflict on a point relating to data protection, this DPA prevails over the Terms of Use and the Terms and Conditions of Sale.
- **Entities on quotation**: the services offered on quotation to sports entities may be subject to additional provisions, specified in the corresponding proposal, which may not reduce the level of protection provided for by this DPA.
- **Amendments**: any substantial amendment to the DPA is notified to the Controller, by e-mail and in the Application, at least thirty days before it takes effect. A Controller who refuses it may stop using the service before that date and export their Records under the conditions of Article 7.8.
- **End**: the termination of the DPA does not affect the deletion and confidentiality obligations, or the export right provided for in Article 7.8.

12. Language, governing law and jurisdiction

This DPA is drafted in French. Translations into English and Dutch are provided for information purposes. **In the event of any discrepancy between the French version and a translation, the French version prevails.**

This DPA is governed by Belgian law. Failing an amicable solution, the courts of the judicial district of Brussels have exclusive jurisdiction, without prejudice to the mandatory rules protecting consumers and to the rights that data subjects derive from Article 79 of the GDPR.

13. Provisions specific to healthcare professionals (Synkro Clinic)

This article applies to a Controller who is a Healthcare Professional, for the entirety of their use of the Application, in accordance with the rule set out in the preamble.

13.1. Purposes

Keeping the Patient's Record; administering standardised questionnaires and clinical tests, with automated score calculation; prescribing and monitoring exercises; exchanges between the Controller and the Patient in the Application; Biomechanical Analysis in support of clinical assessment; artificial intelligence assistance (Article 4.5); management of the calendar, appointments, online appointment booking and reminders; sharing of Records within a Practice; sending the written report to the prescribing doctor and receiving eHealthBox mail; where the Controller has the Administrative Module, the purposes described in Article 13.4.

13.2. Categories of data subjects

- the Controller's Patients;
- the persons who book an appointment online with the Controller, with or without an account;
- where the Administrative Module, the written report or the eHealthBox are used, the prescribing doctors, the doctors holding the global medical record and the senders of the mail received, for the data that identifies them;
- the Practice's administrative staff holding an administrative account, for the data of their account.

13.3. Categories of data

- identification and contact data;
- data concerning health within the meaning of Article 9 of the GDPR: medical history, assessments, session notes, prescriptions, sessions, exercises, alerts and messages exchanged in the Application, confidential information, and the version history of this data;
- written reports sent to the prescribing doctor and mail received in the Controller's eHealthBox (Article 13.4);
- answers to standardised questionnaires and results of clinical tests, including automatically calculated scores and sub-scores;
- videos, images and documents uploaded to the Application, and results of the Biomechanical Analysis;
- appointment data, including, for an online booking without an account, the name, contact details, chosen time slot, any reason for the appointment, answers to the preliminary questionnaire and attachments;
- where the Administrative Module is used, the data listed in Article 13.4.

13.4. Administrative Module (MyCareNet and eHealth platform)

When their offer includes the Administrative Module, the Controller may, from the Application, for the services that are open:

- consult the Patient's insurability with their health insurance fund (MyCareNet Member Data service);
- issue and transmit electronic care certificates (eAttest);
- invoice services to the health insurance funds (eFact);
- request, extend or track medical advisor approvals (eAgreement).

Data processed: social security identification number (NISS); insurability data (health insurance fund, reimbursement codes, special status, third-party payment, community health centre, doctor holding the global medical record); services, session dates, nomenclature codes and amounts; prescription data (date, INAMI (RIZIV) number of the prescriber); approval requests, pathological situations, decisions, approval numbers and reasons for refusal; messages exchanged with the health insurance funds, retained including in their signed raw form, for the purposes of proof and traceability, for the periods required by the regulations of the INAMI (RIZIV) and of the health insurance funds, and at most as long as the Controller's account exists.

Roles and legal bases. Synkro acts as processor of the Controller. The exchanges are carried out in the name of the Controller, on their instruction and by means of their own eHealth certificate, which they upload to the Application and may withdraw at any time; Synkro uses this certificate only to carry out the exchanges that the Controller triggers and to retrieve the responses intended for them during their session, and never stores its password. The Controller bases this processing on Article 9(2)(h) of the GDPR and on the legal obligations incumbent upon them under the regulations on compulsory health care insurance (INAMI (RIZIV)).

Recipients. The health insurance funds, through the MyCareNet network and the eHealth platform. These bodies and platforms act within their own legal framework; they are not sub-processors of

Synkro.

Availability. Each service requires an accreditation. The services are made available one by one, as they open; the Application indicates which services are open. Synkro makes no commitment as to any opening date.

Electronic identity card (eID). Without the Administrative Module being required, the Controller may read a Patient's eID card, by means of a program installed on their computer, in order to pre-fill the Patient's Record. The NISS and the identity data read from the card (surname, first names, date of birth, sex, nationality, address) are processed; the photograph on the card is not recorded.

Written report and eHealthBox. With the same certificate, without the Administrative Module being required, the Controller may send the written report to the prescribing doctor and receive the mail in their eHealthBox (Terms of Use, Article 14.12). The content of the report, its recipient and the eHealthBox acknowledgements are processed, as well as the mail received: sender, Patient concerned and their NISS, text and attachments, encrypted at rest. The mail is incorporated into the Record on the instruction of the Controller.

13.5. Legal bases of the Controller

The Patient's Record is kept under the responsibility of the Controller, a healthcare professional subject to professional secrecy. It is based on Article 9(2)(h) of the GDPR, in compliance with the condition of Article 9(3), and, for its keeping and retention, on the legal obligations of the Controller. The consent that the Patient gives in the Application concerns the use of the Application; its withdrawal ends that use but does not entail the deletion of the Record, the fate of which is a matter for the Controller.

13.6. Professional secrecy

Synkro acknowledges that the Records are covered by the professional secrecy of the Controller. It accesses them only under the conditions of Article 7.2 and does not disclose them to any third party outside the Controller's instructions and the legal obligations that may be binding on Synkro, of which it would inform the Controller under the conditions of Article 7.1.

13.7. Retention of the record

The retention of the Patient's record for the legal period is the responsibility of the Controller, under the conditions of the Terms of Use, Article 14.4. A Record that contains care data is not deleted but made inactive (Terms of Use, Article 13.3). Synkro retains the Records as long as the Controller's account exists and deletes them with it (Article 7.8): it is up to the Controller to export them and to ensure their retention personally.

13.8. Hosting and use in France

The data is hosted in France by Amazon Web Services, which holds Health Data Hosting (HDS) certification for infrastructure hosting. **Synkro itself is not HDS certified.** A Healthcare Professional practising in France assesses, in the light of this information, whether the use of the Application is compatible with the obligations incumbent upon them.

14. Provisions specific to sports professionals (Synkro Motion)

This article applies to a Controller who is not a Healthcare Professional: physical trainer, coach, non-clinical bike fitter, club, federation, performance centre or other sports entity.

14.1. Purposes

Keeping the athlete Record; Biomechanical Analysis of videos; positioning of indicators against published reference standards; comparison of successive readings; sharing of Records within a Team.

14.2. Categories of data subjects

The Athletes monitored by the Controller.

14.3. Categories of data

- identification and contact data;
- sports monitoring data: measurements, observations, discipline, level, session history;
- videos and results of the automated analysis, including aerodynamic estimates;
- where applicable, information revealing data concerning health within the meaning of Article 9 of the GDPR, such as the mention of an injury, of pain or of a return after a period of unavailability.

14.4. Legal bases of the Controller

The Controller bases the processing on the performance of the contract between them and the Athlete or on their legitimate interest in providing the support requested (Articles 6(1)(b) and 6(1)(f) of the GDPR). When the data processed reveals information concerning health, they obtain the explicit consent of the Athlete (Article 9(2)(a) of the GDPR), in compliance, for minors, with the rule of Article 6. The Athlete may withdraw this consent at any time; the Controller then stops the processing that depends on it and deletes the corresponding data, unless there is another legal basis.

14.5. Sports entities and nature of the tool

When an entity (club, federation, centre) organises the monitoring of its Athletes within a Synkro Motion organisation and determines its purposes and means, it is the Controller of the Records concerned, under the conditions of the Terms of Use, Article 15.5.

Synkro Motion is not a medical device, under the conditions of the Terms of Use, Article 15.2.