MEDICAL DATA ADDENDUM

to the FiThrive Customer Terms and Data Processing Agreement (Article 28 GDPR and, where it applies, Article 45 of the Serbian Law on Personal Data Protection)

Processor	FiThrive, Inc., a Delaware corporation, registration number 10727304, with registered office at 131 Continental Dr, Suite 305, 19713, Newark, Delaware, USA – info@fithrive.app
Controller	The organisation identified in the Order Form or in its Online Acceptance under the FiThrive Customer Terms (the 'Organisation')
Agreement supplemented	The agreement between the Organisation and FiThrive, Inc. under the FiThrive Customer Terms, or under an earlier agreement the Organisation has signed with FiThrive, Inc., including the FiThrive Data Processing Agreement and, for an Organisation in the Republic of Serbia, the standard contractual clauses under Serbian law (the 'Agreement')
Applies from	The date on which the Organisation accepts it, by Order Form or by Online Acceptance under the Customer Terms. FiThrive switches the medical features on for the Organisation only from that date.

The Organisation has chosen to use FiThrive's medical features: an injury, illness and availability log kept by the medical staff the Organisation appoints. Medical records are special-category data under Article 9 GDPR and, unlike the rest of the Organisation's content in FiThrive, they are not end-to-end encrypted. This Addendum sets the additional terms on which FiThrive processes them. Where it conflicts with the Agreement, this Addendum prevails for medical data. Terms defined in the Agreement keep their meaning, and the App is the Platform as defined in the Customer Terms.

1. DEFINITIONS

Medical Features – the medical module of the App: medical records, cases, entries, files, athlete self-reports, staff concerns, availability status and history, case sharing, the appointment ledger and the Medical Log.

Medical Data – all personal data processed through the Medical Features, including the content of records and files, availability information, self-reports and concerns, and the Medical Log.

Medical Staff – the coaches, staff members or administrators of the Organisation whom an Organisation administrator appoints in the App to hold medical access for one or more teams.

Availability Information – an athlete's availability status (available, limited, out), expected return date, the existence of an open case, the title of a case shown on the team calendar, the athlete's availability history (intervals and days missed), and the fact that the athlete has reported pain or discomfort, without its content.

Medical Log – the organisation-scoped, append-only record of who opened or changed which record or case, set an availability status, added a file, granted or requested access, exported a record, or appointed or revoked Medical Staff, with actor, subject and time, identifiers only and, for a deleted case, the reason given.

Grant – an athlete's decision in the App to let one named coach, staff member or administrator of their team read one case.

2. ROLES AND INSTRUCTIONS

2.1 Controller and processor. The Organisation is the controller of Medical Data. FiThrive is its processor and processes Medical Data only on the Organisation's documented instructions. The Agreement, this Addendum and the settings the Organisation's administrators make in the App (appointments, team coverage, retention period) are those instructions.

2.2 No processing for FiThrive's own purposes. FiThrive never uses Medical Data for product development, analytics, benchmarking, marketing, training of any model, or any purpose of its own. Aggregate counts that contain no personal data (for example the number of records purged) may be kept for operating the service.

2.3 Not a medical-records system or a medical device. The Organisation acknowledges that the Medical Features are a club's injury and availability log. They are not the record a health professional may be required by law to keep, which remains the professional's responsibility in their own systems, and they do not assess, compute or recommend whether

anyone can train or compete. Every availability status is set by a person the Organisation appointed.

3. THE ORGANISATION'S OBLIGATIONS

3.1 Lawful basis. The Organisation is responsible for the lawfulness of the processing, including the Article 9 condition for health data and any national rules on health data, minors and sports medicine that apply to it. FiThrive gives no assurance that a particular basis is available.

3.2 Appointing Medical Staff. The Organisation shall appoint as Medical Staff only persons who (a) need medical access to perform a medical, physiotherapy or comparable function for the team, and (b) are bound by a statutory duty of professional secrecy or have signed a written confidentiality undertaking at least as strict as Annex 1. The Organisation shall verify qualifications itself; FiThrive does not verify the profession entered in the App. Two Organisation administrators are required where a single administrator wishes to hold medical access, because nobody can appoint themselves. Where the Organisation has only one administrator, it may instead instruct FiThrive in writing to record that administrator's appointment.

3.3 Confidentiality of Medical Staff and management. The Organisation shall ensure that Medical Staff and everyone who receives Availability Information or a Grant: (a) use Medical Data only for the care of the athlete and the planning of training and competition; (b) do not disclose Medical Data to teammates, parents of adult athletes, agents, sponsors, media, other clubs or federations except as the law requires or the athlete agrees; (c) do not use Medical Data in selection, contract or disciplinary decisions beyond the fact of availability; (d) copy or export Medical Data only to keep the professional's own statutory record, and protect any such copy; (e) keep their credentials and second factor personal and do not share devices on which they are signed in; (f) report any suspected misuse or loss to the Organisation at once.

3.4 Transparency towards athletes. The Organisation shall inform its athletes, and the parents or guardians of athletes aged 16 and 17, in its own privacy notice about the Medical Features, including who the Medical Staff are, what coaches see, how sharing works, the retention period it has chosen, that records are not end-to-end encrypted, and that openings

and changes are logged. The in-App notice shown to athletes supplements and does not replace the Organisation's notice.

3.5 Impact assessment and consultation. The Organisation shall assess whether a data protection impact assessment is required before enabling the Medical Features and carry it out where it is. FiThrive provides a support sheet describing the processing, the risks it has identified and the measures in place. Where staff representatives have a right to be consulted on the logging of staff access (for example a works council), the Organisation shall consult them before appointing Medical Staff.

3.6 Retention choice. The Organisation shall choose, in Organisation Settings, how long medical records are kept after an athlete leaves it (2, 5 or 10 years; 5 if it makes no choice) and shall be able to justify the choice. Records are deleted automatically at the end of that period.

3.7 Keeping appointments current. The Organisation shall revoke medical access as soon as a person no longer performs the function for which it was granted. Access is revoked automatically when a person's role drops to athlete, when they leave the Organisation or when their account is erased, but not when they change teams within the Organisation or change function while keeping a coach, staff or administrator role.

3.8 Reviewing the Medical Log. The Organisation shall review the Medical Log at reasonable intervals, and in any case after a complaint, and shall act on any opening or change that had no legitimate purpose.

3.9 Data subject requests. The Organisation handles athletes' requests. Athletes can read their whole record, see who opened or changed it, grant and revoke access, and export their record in the App, as a PDF and, within their account data export, as JSON, without the Organisation's involvement. FiThrive assists with any request the App cannot satisfy within the time limits in the Agreement.

4. FITHRIVE'S OBLIGATIONS

4.1 Access controls. FiThrive keeps the following measures for Medical Data and shall not weaken them without notice under the Agreement's change procedure: (a) every function reserved to Medical Staff requires a session that has completed two-factor authentication, while athletes reach their own record with their ordinary sign-in; (b) no person can read a

record outside the teams they are appointed for, and no one can write to a record without an appointment, enforced in the database for every request; (c) teammates see nothing; coaches, staff and administrators of the team see Availability Information only, and case content only under a Grant; (d) every appointment, revocation, opening and change of a record or case, status change, file added, Grant and export is written to the Medical Log, which no user can edit or delete and whose entries are removed only automatically, together with the record they belong to (clause 4.7); (e) no clinical content is placed in push notifications, in-App notifications, analytics, crash reports or audit metadata.

4.2 Not end-to-end encrypted. The Organisation acknowledges that Medical Data is not end-to-end encrypted. It is stored in the European Union (Frankfurt), encrypted at rest and in transit. Copies of medical files are also held in FiThrive's off-site backup in the European Union, in the same readable form, and medical records form part of the encrypted database backup. This design lets Medical Staff work from any device and prevents the loss of records when a password is forgotten; it is a deliberate choice the Organisation accepts by using the Medical Features.

4.3 FiThrive personnel. FiThrive personnel cannot reach Medical Data through the App or through FiThrive's internal tools. Administrator access to the database at the hosting level is used for Medical Data only (a) on the Organisation's written instruction, or (b) where strictly necessary to restore the service or to investigate a security incident. Every such access is recorded and reported to the Organisation within the time limit in clause 4.6. FiThrive personnel with such access are bound by written confidentiality obligations.

4.4 Sub-processors. Medical Data is processed by the following sub-processors, in the roles stated: Supabase (database, file storage and functions, AWS eu-central-1, Frankfurt); Cloudflare (off-site backup storage, R2, European Union); Google/Firebase and Apple (delivery of push notifications containing an athlete's name with fixed wording – for example the availability status and expected return date, that the athlete reported pain or discomfort, or that a case was shared – never a diagnosis, body area or record text); GitHub (runs the backup job, through which the database export and the files pass; keeps no copy). Changes follow the sub-processor procedure in the Agreement.

4.5 Transfers. FiThrive is established in the United States; its personnel administer the service from the Republic of Serbia and, for executive management, from the Republic of Slovenia. The Standard Contractual Clauses in the Agreement cover Medical Data. Because

Medical Data is readable at the database level, FiThrive applies the access restriction in clause 4.3 as a supplementary measure.

4.6 Incident notification. FiThrive shall notify the Organisation of a personal data breach affecting Medical Data without undue delay and no later than 48 hours after becoming aware of it, with the information Article 33(3) GDPR requires as far as it is available, and shall update the notice as facts are established.

4.7 Retention and deletion. FiThrive deletes a medical record, its files and its log rows automatically 2, 5 or 10 years after the athlete leaves the Organisation, as configured, and immediately when the athlete's account is erased. When Medical Staff delete a case, the case and its files are deleted at once; the record remains and the Medical Log keeps the entry of that deletion. Copies of deleted medical files are removed from the off-site backup within 30 days. Medical Data inside encrypted database backups expires with the backup schedule (at most 12 months) and any deletion is re-applied after a restore. On termination of the Agreement FiThrive deletes the Organisation's Medical Data together with its other data, as the Agreement provides; the retention period under clause 3.6 runs only while the Agreement is in force. The Organisation shall export what it must keep before termination.

4.8 Assistance and audit. FiThrive assists the Organisation with impact assessments, prior consultation, data subject requests and breach notifications concerning Medical Data, and makes the Medical Log available to the Organisation's administrators in the App at all times. The audit rights of the Agreement apply.

5. MINORS

5.1 Age. The App admits nobody under 16. For athletes aged 16 and 17 the Organisation holds the parental consent confirmed at invitation under the Agreement.

5.2 Athlete control. Athletes of any age read their own record and decide themselves which cases to share. Medical Staff cannot grant access on an athlete's behalf. Where the law of the Organisation's country requires a parent or guardian to decide for a 16- or 17-year-old, the Organisation shall obtain that decision outside the App and instruct FiThrive in writing.

6. LIABILITY, TERM AND PRECEDENCE

6.1 Liability. The liability provisions of the Agreement apply to this Addendum without change.

6.2 Term. This Addendum applies from the date in the table above and remains in force while FiThrive holds any Medical Data of the Organisation, including in backups until they expire.

6.3 Precedence. For Medical Data this Addendum prevails over the Agreement; the Standard Contractual Clauses prevail over both where the law so requires.

ANNEX 1 – CONFIDENTIALITY UNDERTAKING FOR MEDICAL STAFF (TEMPLATE)

For use by the Organisation under clause 3.2(b) where the appointee is not already bound by a statutory duty of professional secrecy. One signed copy is kept by the Organisation.

I, [full name], appointed by [Organisation] as medical staff for [team(s)] in the FiThrive App, undertake that:

1. I will open, read and change athletes' medical records only to care for the athlete and to inform training and competition planning.
2. I will not disclose anything from a medical record to teammates, parents of adult athletes, agents, sponsors, media, other clubs or federations, except as the law requires or the athlete has agreed.
3. I will set an athlete's availability on my own professional judgement and record the reason in the case.
4. I will choose case titles that do not reveal a diagnosis, because the title is visible to the team's coaches and administrators on the calendar.
5. I will export or copy a record only to keep my own statutory professional record, and I will protect that copy.
6. I will keep my password and second factor to myself and lock or sign out of shared devices.
7. I understand that every opening and change I make is logged with my name and is visible to the Organisation's administrators and to the athlete.
8. I will report any suspected misuse, loss or wrongful disclosure to the Organisation immediately.
9. These duties continue after my appointment ends.

Medical staff member	**For the Organisation**
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____
Signature: _____	Signature: _____