

Accordo sul trattamento dei dati

L'accordo dell'art. 28 GDPR fra la palestra e Ghisa Pro.

FORNITORE Viola Fabrizio, ditta individuale Partita IVA 03959520929 · REA CA-352250	SEDE Via Petrarca 24/E1 09017 Sant'Antioco (SU)
CONTATTI info@ghisapro.com palestre.ghisapro.com	DOCUMENTO Versione 2.2 del 6 ottobre 2026. Si accetta insieme alle Condizioni di servizio.

INDICE

Le parti

- 1 Oggetto e durata
- 2 Natura e finalità del trattamento
- 3 Istruzioni documentate
- 4 Riservatezza e chi può accedere
- 5 Le misure di sicurezza (art. 32)
- 6 Sub-responsabili
- 7 Aiuto sui diritti degli interessati
- 8 Aiuto sugli obblighi degli articoli da 32 a 36
- 9 Violazioni dei dati: ti avvisiamo entro 24 ore
- 10 Cosa succede ai dati alla fine

- 11 Audit e informazioni
 - 12 Trasferimenti fuori dall'Unione europea
 - 13 Il caso del cliente che ti dà il consenso dall'app
- Allegato I** Cosa trattiamo, per chi, e per quanto
- Categorie di interessati
- Tipi di dati personali — rubrica degli iscritti
- Tipi di dati personali — altri trattamenti
- Natura e durata
- Allegato II** Misure di sicurezza
- Allegato III** Sub-responsabili autorizzati
- Allegato IV** Istruzioni di sicurezza per te

Questo accordo regola il modo in cui trattiamo, **per conto tuo**, i dati personali dei tuoi iscritti e dei tuoi clienti che finiscono nel pannello **palestre.ghisapro.com**. Lo impone l'art. 28, paragrafo 3, del Regolamento (UE) 2016/679: senza un accordo scritto non potremmo trattare quei dati, e tu non potresti affidarceli. Segue le clausole contrattuali tipo adottate dalla Commissione europea con la **Decisione di esecuzione (UE) 2021/915 del 4 giugno 2021**, scritte in italiano corrente.

L'accordo è parte integrante delle *Condizioni di servizio del pannello Ghisa Pro per palestre e personal trainer* e si accetta insieme a quelle, al momento della registrazione o al primo accesso. Registriamo la versione accettata, la data, l'ora, l'indirizzo IP, il browser e l'impronta digitale (SHA-256) dei due documenti. L'accettazione per via elettronica soddisfa la forma scritta richiesta dall'art. 28, paragrafo 9.

Le parti

Titolare del trattamento: la palestra, il centro sportivo, l'associazione o il personal trainer che si registra al pannello, come identificato dai dati inseriti in fase di registrazione e nei dati di fatturazione (nome, città, email, telefono, ragione sociale, partita IVA o codice fiscale). Nel testo: «tu».

Responsabile del trattamento: Viola Fabrizio, ditta individuale, partita IVA **03959520929**, sede in **Via Petrarca 24/E1, 09017 Sant'Antioco (SU)**, email **info@ghisapro.com**, posta elettronica certificata risultante dal Registro delle imprese. Nel testo: «noi».

Sei tu il titolare perché sei tu a decidere di tenere una rubrica degli iscritti, chi inserirci, quali campi compilare, per quanto tempo conservarli e quando cancellarli: decidi le finalità e i mezzi essenziali del trattamento (art. 4, punto 7). Noi forniamo il software e lo ospitiamo, e non usiamo quei dati per nessuna finalità nostra: siamo responsabili del trattamento (art. 4, punto 8).

1 Oggetto e durata

Trattiamo per conto tuo i dati personali descritti nell'**Allegato I**, con le modalità descritte in questo accordo, per il solo scopo di farti funzionare il pannello.

L'accordo dura quanto dura il tuo contratto di servizio e cessa con esso. Gli obblighi che per loro natura sopravvivono — riservatezza, cancellazione o restituzione dei dati, assistenza su fatti avvenuti prima della cessazione — restano in vita anche dopo.

2 Natura e finalità del trattamento

Le operazioni che compiamo sono: **raccolta** (tramite i moduli del pannello), **registrazione e conservazione** su banca dati, **consultazione** limitata ai casi del punto 4, **modifica e cancellazione** su tua richiesta o per tua azione, **estrazione** per fornirti copia dei dati quando ce la chiedi, **trasmissione** al solo interessato, nella sua app, delle schede che gli condividi e dei suoi propri dati, e **copia di sicurezza**.

Le finalità sono quelle del pannello, e solo quelle: farti gestire la rubrica dei tuoi iscritti; i loro abbonamenti e servizi con le rate, gli incassi e le ricevute di pagamento; il registro degli ingressi, anche con il codice QR; i corsi con le prenotazioni; le schede di allenamento da assegnare ai clienti che ti hanno abilitato nell'app; gli accessi dei tuoi dipendenti con i loro permessi; le notifiche su quello che succede nel tuo account; mostrare a ciascun iscritto che hai collegato alla sua app **i suoi propri dati** (abbonamenti, rate, scadenze, certificato, corsi e prenotazioni, pass d'ingresso).

Non usiamo quei dati per altro. Non li leggiamo per farci statistiche, non li usiamo per addestrare modelli, non li cediamo, non li mostriamo ad altre palestre e non li usiamo per venderti niente. Nell'app arrivano soltanto alla persona a cui si riferiscono, e mai le patologie. Dei tuoi dipendenti, all'iscritto arrivano soltanto nome e cognome degli istruttori dei corsi che pubblichi nell'app e di chi ha scritto le schede che gli mandi.

3 Istruzioni documentate

Trattiamo i dati personali **soltanto su tua istruzione documentata**, anche per quanto riguarda gli eventuali trasferimenti verso paesi terzi (art. 28, par. 3, lett. a).

Le tue istruzioni documentate sono, insieme: questo accordo con i suoi allegati; le condizioni di servizio; e le azioni che compi dentro il pannello, che sono istruzioni a tutti gli effetti — quando scrivi un iscritto ci stai istruendo a conservarlo, quando lo cancelli ci stai istruendo a cancellarlo. Istruzioni ulteriori puoi darcele per iscritto a **info@ghisapro.com**; ci riserviamo di dirti se un'istruzione è tecnicamente impossibile o se richiede un costo, e in tal caso ne parliamo prima.

Possiamo trattare i dati oltre le tue istruzioni solo se ce lo impone il diritto dell'Unione o italiano: in quel caso te lo comunichiamo prima di procedere, a meno che la stessa legge non lo vieti per motivi di interesse pubblico.

Se riteniamo che una tua istruzione violi il Regolamento, te lo diciamo subito e per iscritto, e sospendiamo l'esecuzione di quella istruzione finché non la ritiri o non la chiarisci (art. 28, par. 3, ultimo capoverso). Per esempio: se ci chiedessi di esportarti i carichi, lo storico degli allenamenti o i dati corporei dei tuoi clienti dell'app, rifiuteremmo per iscritto.

4 Riservatezza e chi può accedere

Il progetto è portato avanti da una sola persona fisica, che con questo accordo si impegna **personalmente alla riservatezza** su tutti i dati trattati per tuo conto, con un impegno che resta in vigore anche dopo la fine del rapporto (art. 28, par. 3, lett. b).

Non accediamo ai dati dei tuoi iscritti, salvo in tre casi, tutti circoscritti: quando ci chiedi tu assistenza e l'accesso serve a darla, e per il tempo che serve; quando è indispensabile per diagnosticare un guasto che impedisce al servizio di funzionare; quando ce lo impone la legge o un'autorità. Gli accessi per assistenza si fanno, quando è tecnicamente possibile, su dati ridotti al minimo necessario.

Se in futuro altre persone collaboreranno al progetto, saranno vincolate per iscritto allo stesso obbligo di riservatezza prima di poter accedere a qualunque dato, e riceveranno solo gli accessi necessari al loro compito.

5 Le misure di sicurezza (art. 32)

Queste sono le misure **in vigore oggi** nel software che stai usando. Se una misura viene ridotta te lo comunichiamo come modifica dell'accordo; possiamo invece migliorarle in qualunque momento.

Isolamento per palestra (la misura principale). Ogni dato porta l'identificativo della palestra a cui appartiene, e la banca dati stessa — non solo il programma — consente di leggerlo e scriverlo soltanto a quella palestra: al titolare e ai dipendenti a cui il titolare ha dato l'accesso. La palestra si ricava da chi è entrato, mai da ciò che chiede il browser. È ciò che impedisce a un'altra palestra di vedere i tuoi iscritti. Vale per iscritti, abbonamenti, rate, ingressi, corsi, prenotazioni, dipendenti, schede, consensi e notifiche.

Accessi personali con permessi. Ogni dipendente entra con un nome utente e una password suoi; la password del primo accesso va cambiata subito e da quel momento non è conservata in chiaro. Ognuno vede e fa solo ciò che i suoi permessi consentono, e il controllo avviene sul server: senza il permesso «dati sanitari» le patologie non arrivano nemmeno al browser. Un accesso disattivato smette di funzionare subito.

Cestino e cancellazione. Un iscritto eliminato resta 30 giorni in un cestino, invisibile a tutto il resto del pannello e all'app, poi è cancellato automaticamente; la cancellazione immediata e definitiva la può fare solo il titolare.

Registro degli scaricamenti. Ogni esportazione di dati dal pannello è annotata con chi l'ha fatta e quando, e l'annotazione resta 24 mesi.

Nessuna lettura anonima. Non esiste un modo di leggere quei dati senza essere autenticati. Le operazioni delicate passano da funzioni sul server, che rifanno ogni controllo e non si fidano di quello che chiede il browser. I tentativi di accesso sono limitati in frequenza. L'area di amministrazione del servizio è separata dal pannello ed è protetta, oltre che dalla password, da un **secondo fattore** (codice da un'app di autenticazione), attivo sull'account di chi amministra il servizio.

Cifratura in transito. Tutte le connessioni fra il tuo browser, il pannello e la banca dati viaggiano cifrate (HTTPS/TLS). I dati a riposo sono protetti dalla cifratura del disco applicata dal fornitore della banca dati.

Nessun codice di terze parti. Nel pannello non gira nessuno strumento di analisi, di tracciamento o di pubblicità, e i caratteri tipografici sono serviti dal nostro server. I soli indirizzi a cui la pagina manda dati sono **la nostra banca dati e il nostro server**. Quando scegli o paghi il **tuo** piano, il browser va sulla pagina di Stripe: è un cambio di pagina

per il pagamento del tuo abbonamento, e non porta con sé nessun dato dei tuoi iscritti. Il pannello dichiara al browser le sole destinazioni ammesse (Content-Security-Policy) e il browser **blocca** tutte le altre; la pagina non può nemmeno essere incorporata in siti altrui.

WhatsApp ed email: un canale che scegli tu. Accanto al link personale di un iscritto, al suo codice d'ingresso e alle credenziali di un dipendente il pannello offre i pulsanti **WhatsApp** ed **Email**. Toccandoli, il pannello apre WhatsApp (passando dall'indirizzo **wa.me** di Meta, con il numero e il testo dentro l'indirizzo) o il programma di posta del tuo dispositivo, con il messaggio già scritto; l'invio lo fai tu. È un canale di comunicazione fra te e i tuoi iscritti o dipendenti, scelto da te come titolare: da lì valgono le condizioni di WhatsApp (Meta) o del tuo servizio di posta, e Meta non è un nostro sub-responsabile. Per le credenziali e il codice d'ingresso, che servono a entrare, valuta tu se usare un canale diverso (a voce, di persona, con la tessera stampata).

Separazione verso l'app. Dal pannello all'app viaggiano solo le schede che condividi e, verso l'iscritto che hai collegato alla sua app, **i suoi propri dati**: abbonamenti, rate, scadenze, certificato consegnato e sua scadenza, corsi e prenotazioni, pass d'ingresso, con nome e cognome dell'istruttore che tiene il corso o ha scritto la scheda. Mai le patologie, mai i dati di un altro iscritto. In senso inverso, al pannello arrivano dai clienti che ti abilitano solo i dati elencati al punto 6 delle condizioni (soprannome, foto, date, avvisi, prenotazioni, struttura delle schede): mai carichi, storico, massimali o misure corporee. Esistono test automatici che lo verificano a ogni modifica.

Copie di sicurezza cifrate. Le copie di sicurezza sono cifrate con AES-256 e conservate su **Google Drive** (vedi Allegato III); la cifratura avviene prima che la copia lasci i nostri dispositivi, e la chiave di cifratura e la chiave di accesso alla banca dati sono tenute fuori dal codice: Google custodisce file che non può leggere. Ogni copia è completa e datata e non viene sovrascritta dalla successiva; le eliminiamo a mano, con un controllo almeno una volta al mese, così che nessuna copia superi i **12 mesi**.

Aggiornamenti e verifica. Le librerie di terze parti usate dal pannello sono fissate a una versione esatta e servite dal nostro server, non prelevate da distributori esterni. Prima di ogni pubblicazione gira una serie di test automatici.

Il rischio che resta, e che devi conoscere

Il pannello è un'applicazione web e, come ogni applicazione web, **tiene nel browser del tuo computer i dati che ti sta mostrando**, patologie comprese. Chi si siede davanti a quel computer mentre è sbloccato li legge. È una caratteristica di ogni applicazione web, che le nostre misure non possono eliminare: le misure che la governano sono le tue, e le trovi nell'**Allegato IV**.

Quello che oggi il pannello non fa ancora: non blocca automaticamente la sessione dopo un periodo di inattività, e all'uscita non azzerava tutto ciò che ha tenuto in memoria. Sono due misure in programma; nel frattempo valgono le istruzioni dell'**Allegato IV**.

Non offriamo la cifratura dei dati a riposo con una chiave in tuo esclusivo possesso: renderebbe impossibili la ricerca per nome e i filtri del gestionale, e comporterebbe la perdita totale dei dati se smarrissi la chiave.

6 Sub-responsabili

Ci autorizzi in via **generale** a ricorrere ai sub-responsabili elencati nell'**Allegato III** (art. 28, par. 2). A ciascuno, **tranne Google**, imponiamo per contratto gli stessi obblighi di protezione dei dati che valgono per noi, e **restiamo pienamente responsabili verso di te** del loro operato, Google compreso (art. 28, par. 4).

Google, detto com'è. Le copie di sicurezza stanno su Google Drive di un account Google personale, e per quel tipo di account Google non sottoscrive un accordo sul trattamento dei dati: lo offre solo con i suoi servizi per le aziende. Per questo le copie partono **già cifrate** con AES-256 e la chiave resta a noi: Google custodisce file che non può leggere, e non ha accesso in chiaro a nessun dato dei tuoi iscritti. È un punto che intendiamo regolarizzare (con il servizio di Google per le aziende e il suo accordo, o spostando le copie da un altro fornitore): il cambio ti sarà comunicato come ogni cambio di sub-responsabile.

Se vogliamo aggiungerne o sostituirne uno, te lo comunichiamo per email con **almeno 30 giorni di preavviso**, dicendo chi è, cosa farà e dove si trova. Entro quel termine puoi **opporti** per motivi ragionevoli legati alla protezione dei dati, scrivendo a info@ghisapro.com. Se l'opposizione è fondata e non troviamo una soluzione alternativa, puoi **recedere** dal servizio senza costi e con diritto a ricevere copia dei dati secondo le condizioni di servizio.

Uno dei nostri fornitori ci concede a sua volta un preavviso più breve (14 giorni). Se il cambio riguarda lui, ti avvisiamo appena lo sappiamo, e il tuo diritto di opposti e di recedere vale comunque per 30 giorni dalla nostra comunicazione, anche se il cambio a monte avviene prima.

I nostri sub-responsabili si appoggiano a loro volta ad altri fornitori (per rete, archiviazione e registri): ciascuno pubblica il proprio elenco, che trovi nell'Allegato III.

7 Aiuto sui diritti degli interessati

I tuoi iscritti hanno i diritti degli articoli da 15 a 22 del Regolamento, e li esercitano **verso di te**, che sei il titolare. Se una richiesta arriva a noi per sbaglio, **non rispondiamo nel merito**: te la giriamo senza indebito ritardo e in ogni caso **entro 5 giorni lavorativi**, e ti diciamo che l'abbiamo ricevuta.

Ti assistiamo con misure tecniche e organizzative adeguate perché tu possa rispondere nei termini dell'art. 12 (art. 28, par. 3, lett. e). In concreto: il pannello ti permette già di **vedere, correggere e cancellare** da solo ogni riga della rubrica, e questo copre da sé la maggior parte delle richieste di accesso, rettifica e cancellazione (per la cancellazione: «Elimina» e poi, dal cestino, «Elimina definitivamente», riservato al titolare). Per la portabilità dell'art. 20 c'è «Scarica i suoi dati» nella pagina dell'iscritto. Se preferisci che la copia la prepariamo noi — per esempio per rispondere a una richiesta di portabilità — ce la chiedi e te la mandiamo entro 15 giorni, in JSON o CSV, senza costi. Lo stesso vale per qualunque richiesta che non si risolva con le funzioni del pannello, salvo che le richieste diventino manifestamente eccessive.

8 Aiuto sugli obblighi degli articoli da 32 a 36

Ti assistiamo, tenendo conto della natura del trattamento e delle informazioni di cui disponiamo, nel rispetto degli obblighi di sicurezza (art. 32), di notifica e comunicazione delle violazioni (artt. 33 e 34), di valutazione d'impatto (art. 35) e di consultazione preventiva dell'autorità (art. 36).

In pratica: le informazioni tecniche di questo accordo, e in particolare il punto 5 e gli Allegati, sono scritte per poter essere copiate dentro la tua valutazione d'impatto. Se stai facendo una valutazione d'impatto e ti serve un dettaglio che qui non c'è, chiedicelo.

9 Violazioni dei dati: ti avvisiamo entro 24 ore

Se veniamo a conoscenza di una violazione di sicurezza che riguarda i dati personali trattati per conto tuo, **te lo comunichiamo senza ingiustificato ritardo e comunque entro 24 ore** dal momento in cui ne veniamo a conoscenza, all'indirizzo email del tuo account (art. 28, par. 3, lett. f, e art. 33, par. 2).

La notifica al Garante spetta a **te**, entro 72 ore (art. 33, par. 1): per questo il nostro termine è breve.

Nella comunicazione ti diamo tutte le informazioni dell'art. 33, par. 3, che siamo gli unici ad avere: la natura della violazione, le **categorie e il numero approssimativo di interessati** e di record coinvolti, le **conseguenze probabili**, le **misure adottate** per porvi rimedio e attenuarne gli effetti, e un punto di contatto per i dettagli. Se non abbiamo ancora tutte le informazioni, ti diamo quelle che abbiamo e ti aggiorniamo man mano.

Non notificiamo noi al Garante e non contattiamo noi i tuoi iscritti: la valutazione del rischio e le comunicazioni spettano a te, che sei il titolare. Se ci chiedi aiuto per redigerle, te lo diamo.

Documentiamo ogni violazione — circostanze, conseguenze, decisioni prese — in un registro interno, e te ne diamo copia per la parte che ti riguarda se te ne serve.

10 Cosa succede ai dati alla fine

Alla cessazione del servizio, **su tua scelta**, cancelliamo o ti restituiamo tutti i dati personali trattati per conto tuo (art. 28, par. 3, lett. g).

Concretamente: dal pannello puoi esportare tutto da solo, in qualunque momento e anche a servizio sospeso o in sola lettura: la pagina **Backup** ti dà tutti i dati in un file (CSV per ogni area e JSON completo), e dalla pagina di ogni iscritto scarichi i suoi. Se preferisci che la copia la prepariamo noi, ce la chiedi e te la mandiamo entro 15 giorni in un formato leggibile da un programma.

Quando il tuo piano finisce i dati restano dove sono, in sola lettura, per **almeno 90 giorni**. Trascorso quel termine possiamo cancellarli, avvisandoti per email con **almeno 30 giorni di anticipo**. Se chiedi tu la cancellazione, **cancelliamo tutto** dalla banca dati senza attendere. È la stessa regola del punto 14 delle condizioni di servizio.

Le copie di sicurezza cifrate sono file completi e datati e non si sovrascrivono fra loro: i dati cancellati restano nelle copie già prese finché non eliminiamo quelle copie. Le eliminiamo a mano, con un controllo almeno una volta al mese, così che nessuna copia superi i **12 mesi**. Se la legge ci impone di conservare qualcosa, te lo diciamo e conserviamo solo quello, per il tempo imposto e senza usarlo per altro.

I tempi di conservazione durante il rapporto

I tempi li decidi tu, che sei il titolare, ma il pannello è costruito intorno a questi, che riteniamo difendibili e che ti consigliamo di adottare e di dichiarare nella tua informativa:

I **dati anagrafici e di abbonamento** (nome, cognome, cellulare, data di nascita, email, foto, abbonamento e scadenza, pagamento) si tengono finché il rapporto è in corso, e dopo la fine solo per quanto serve a documentarlo: al massimo **10 anni** per quello che ha rilievo contabile (artt. 2220 e 2946 del codice civile), ma **due o tre anni** sono il termine ragionevole per foto e cellulare, che alla contabilità non servono.

Il **certificato medico e le patologie** si tengono **un anno dalla scadenza del certificato**, o fino alla fine del rapporto se prima; la revoca del consenso li cancella subito. Qui il termine lungo non si giustifica: la finalità è sapere chi è in regola oggi.

Le **schede assegnate** si tengono finché dura il rapporto e per **un anno** dopo, perché un cliente che torna ritrovi il suo programma. Le **notifiche** del pannello si cancellano da sole **90 giorni** dopo la loro data; quelle già lette puoi cancellarle tu prima, dalla pagina Notifiche.

Gli **ingressi e le uscite** servono a controllare gli accessi e a gestire i carnet: dopo **12 mesi** dalla registrazione non servono più. Il **codice d'ingresso** vale fino alla fine dell'iscrizione.

Le **rate, gli incassi e le ricevute** hanno rilievo contabile: fino a **10 anni** dalla fine del rapporto, come i dati di abbonamento.

Le **prenotazioni ai corsi**: **12 mesi** dalla lezione. Gli **avvisi** ai clienti dell'app (lezione spostata o annullata, prenotazione fatta o tolta) si cancellano da soli **12 mesi** dopo l'avviso.

Il **registro delle esportazioni** serve a sapere chi ha portato fuori dei dati: si cancella da solo **24 mesi** dopo ogni scaricamento.

Sui **consensi dei clienti dell'app**, che gestiamo noi: la banca dati tiene **una sola riga per ogni coppia cliente-palestra**, con la data del consenso e, se c'è stata, quella della revoca; se il cliente revoca e poi riacconsente, la riga viene riscritta. Ogni consenso e ogni revoca, però, e così ogni associazione col link personale e ogni scollegamento, generano anche un **avviso datato** nelle notifiche del tuo pannello: quegli avvisi sono la traccia storica, e come tutte le notifiche si cancellano da soli **90 giorni** dopo la loro data (prima, se li cancelli tu dopo averli letti, o se il cliente

cancella il suo account: in quel caso spariscono con lui). Non teniamo noi un archivio separato dei consensi. Se ti serve una prova datata di un consenso o di una revoca oltre quel termine, annotala tu (per esempio salvando una schermata dell'avviso) o chiedicela finché l'avviso c'è.

Al maturare dei termini il pannello cancella **da solo**, con un controllo che gira ogni notte, soltanto queste cose: le notifiche dopo 90 giorni, gli avvisi ai clienti dell'app dopo 12 mesi, il registro delle esportazioni dopo 24 mesi; e, dopo 30 giorni, ciò che hai messo tu nel cestino. Tutto il resto **non lo cancella da solo**: la cancellazione è un'azione tua, e resta un tuo obbligo di titolare.

11 Audit e informazioni

Ti mettiamo a disposizione tutte le informazioni necessarie a dimostrare il rispetto dell'art. 28 e consentiamo e contribuiamo alle attività di revisione, comprese le ispezioni, svolte da te o da un incaricato che designi (art. 28, par. 3, lett. h).

In pratica: rispondiamo per iscritto alle tue domande sulla sicurezza e sul trattamento **entro 15 giorni**. Se vuoi svolgere una verifica più approfondita, ci accordiamo sui tempi con almeno 30 giorni di preavviso, non più di una volta l'anno salvo che sia avvenuta una violazione o che un'autorità te lo imponga, con obbligo di riservatezza su quello che vedi e senza che la verifica interferisca con il servizio degli altri clienti o esponga i loro dati.

Ti informiamo subito se, a nostro giudizio, un'istruzione che ci dai o una richiesta che ci fai viola il Regolamento o un'altra norma sulla protezione dei dati.

12 Trasferimenti fuori dall'Unione europea

I dati sono conservati nella regione di **Francoforte, in Germania**, quindi **all'interno dell'Unione europea**. Le email di servizio partono da un'infrastruttura nella regione **Irlanda**.

I nostri fornitori però non sono società europee, e il loro personale può, in casi limitati e per attività di assistenza e manutenzione, accedere ai dati da fuori dell'Unione; Resend dichiara inoltre che il proprio trattamento avviene principalmente negli Stati Uniti. Questo è un trasferimento ai sensi del capo V del Regolamento. Lo strumento che lo copre, fornitore per fornitore:

FORNITORE	PAESE	STRUMENTO DI TRASFERIMENTO
Supabase Pte. Ltd.	Singapore	Clausole contrattuali tipo (Decisione di esecuzione (UE) 2021/914), moduli due e tre, incorporate nel suo accordo sul trattamento. Per Singapore non esiste una decisione di adeguatezza.
Cloudflare, Inc.	Stati Uniti	Certificazione nel quadro UE-Stati Uniti per la protezione dei dati (decisione di adeguatezza (UE) 2023/1795); in subordine, clausole contrattuali tipo incorporate nel suo accordo.
Plus Five Five, Inc. (Resend)	Stati Uniti	Clausole contrattuali tipo incorporate nel suo accordo; in aggiunta, certificazione nel quadro UE-Stati Uniti.
Google LLC	Stati Uniti	Certificazione nel quadro UE-Stati Uniti . Nessun accordo sul trattamento (punto 6). Riceve soltanto file cifrati, di cui non possiede la chiave.

A questi strumenti si aggiungono le misure supplementari dichiarate da ciascun fornitore (cifratura in transito e a riposo, procedure per le richieste delle autorità, rapporti di trasparenza). Le certificazioni sono state verificate alla data di questa versione; l'elenco ufficiale è pubblico su <https://www.dataprivacyframework.gov/list>.

Non trasferiamo dati verso paesi diversi da quelli indicati qui e nell'Allegato III. Se questo dovesse cambiare, vale il preavviso di 30 giorni del punto 6.

13 Il caso del cliente che ti dà il consenso dall'app

Quando un utente dell'app ti dà il consenso, siamo **noi** a comunicarti il suo soprannome, la sua foto e gli altri dati elencati al punto 6 delle condizioni, e lo facciamo come **titolari** di quei dati, su richiesta esplicita del nostro utente, sulla base del consenso che ha prestato nell'app e che resta registrato con la data. Di quella comunicazione rispondiamo noi, e l'utente può revocarla in qualunque momento dall'app: da quel momento sparisce dal tuo elenco.

Da quando quei dati sono nelle tue mani, **sei tu a decidere cosa farne** — se assegnare una scheda, quale, quante volte aggiornarla —, e per quella parte sei titolare e noi torniamo a essere i tuoi responsabili, alle stesse condizioni di questo accordo.

Ne discende che nessuno dei due è «contitolare» dell'altro, e che ciascuno risponde del proprio pezzo. Perché l'interessato non resti in mezzo, ci impegniamo a indicargli te come referente per tutto ciò che riguarda l'uso che fai dei suoi dati, e tu ti impegni a indicare noi per la parte dell'app. Il punto di contatto comune è **info@ghisapro.com**: qualunque richiesta arrivi lì e riguardi te, te la giriamo entro 5 giorni lavorativi.

Cosa trattiamo, per chi, e per quanto

Categorie di interessati

Le **persone iscritte alla tua palestra o tue clienti**, inserite da te nella rubrica. Non sono necessariamente utenti dell'app: sono clienti tuoi e basta.

Gli **utenti dell'app che ti hanno dato il consenso**, per i dati elencati più sotto («Clienti dell'app con consenso»).

Gli **iscritti minorenni**. Per loro l'informativa e i consensi (in particolare quelli sul certificato e sulle patologie) li firma **un genitore o chi esercita la responsabilità genitoriale**, e raccoglierli resta compito tuo. Il pannello non ha campi dedicati al genitore: se ne annoti i dati (per esempio per una ricevuta), anche quelli sono trattati per tuo conto alle stesse condizioni.

I **tui dipendenti e collaboratori** a cui crei un accesso al pannello: nome, cognome, data di nascita, cellulare, email, mansione, nome utente, permessi, i corsi che tengono. Nome e cognome di chi tiene un corso pubblicato nell'app o ha scritto una scheda compagno nell'app degli iscritti collegati che vedono quel corso o ricevono quella scheda.

Tipi di dati personali — rubrica degli iscritti

DATO	OBBLIGATORIO	NOTE
Nome	sì	
Cognome	sì	
Cellulare	sì	
Data di nascita	sì	
Email	no	
Codice fiscale	no	serve alle ricevute
Residenza (via, civico, CAP, città)	no	serve alle ricevute
Foto	no	immagine ridotta a 320 pixel prima dell'invio
Data di iscrizione	no	
Istruttore di sala	no	
Abbonamenti e servizi	no	tipo, inizio, scadenza, ingressi del carnet
Rate e incassi	no	importo, scadenza, data e metodo del pagamento, numero della ricevuta; promemoria, non documento fiscale
Ingressi	no	data e ora di entrata e uscita, se registrati a mano o con il QR
Codice del pass d'ingresso (QR)	automatico	casuale, rigenerabile
Prenotazioni ai corsi	no	
Certificato medico consegnato (sì/no)	no	dato relativo alla salute, art. 9

DATO	OBBLIGATORIO	NOTE
Scadenza del certificato medico	no	dato relativo alla salute, art. 9
Patologie (testo libero, max 600 caratteri)	no	dato relativo alla salute, art. 9
Collegamento all'utente dell'app	no	solo se la persona ha usato il suo link personale
Blocco e sblocco dell'ingresso	no	

Il pannello non conserva il file del certificato medico: solo il fatto che esista e quando scade. È una scelta di minimizzazione (art. 5, par. 1, lett. c): il documento contiene la diagnosi, il nome del medico e altro che alla tua finalità non serve.

Certificato e patologie sono categorie particolari di dati ai sensi dell'art. 9, par. 1. **Questo servizio ti chiede di compilare quei campi solo dopo aver raccolto il consenso esplicito** dell'interessato, in modo **separato** per ciascuno dei due (art. 9, par. 2, lett. a). È una regola d'uso del pannello, scelta per prudenza: la valutazione della base giuridica del tuo trattamento resta tua. I moduli pronti sono in fondo al modello di informativa. Nel campo «patologie» scrivi solo l'indicazione operativa che ti serve in sala: non una diagnosi, non un referto, mai informazioni su altre persone.

Tipi di dati personali — altri trattamenti

Clienti dell'app con consenso: identificativo tecnico, soprannome, foto del profilo, data del consenso e dell'eventuale revoca, numero di schede assegnate e nome di quella condivisa, avvisi datati (consenso, revoca, associazione col link personale, scollegamento, scheda rimandata o eliminata), prenotazioni fatte dall'app (una prenotazione disdetta sparisce), collegamento all'iscritto se ha usato il link personale. **Mai** carichi, storico, massimali, peso, misure corporee, dati nutrizionali, data di nascita o email.

Schede di allenamento: nome della scheda, sedute, esercizi, serie, ripetizioni, recuperi, carichi prescritti, note, categoria, istruttore che l'ha scritta, gli esercizi creati dalla tua palestra.

Registro delle esportazioni: chi del tuo personale ha scaricato quali dati, e quando; cancellato in automatico dopo 24 mesi.

Avvisi ai clienti dell'app: lezione spostata o annullata, prenotazione fatta o tolta dalla palestra, con la data; cancellati in automatico dopo 12 mesi.

Notifiche del pannello: gli avvisi che ricevi (consensi, revoche, associazioni, scollegamenti, schede rimandate o eliminate dai clienti), cancellati in automatico dopo 90 giorni; quelli letti puoi cancellarli prima.

Ricevute di pagamento (se le usi): il documento viene creato sul tuo dispositivo e lo conservi tu. Sui nostri sistemi restano il numero assegnato e la copia dei dati stampati — nome, codice fiscale e residenza dell'iscritto, importo, data e metodo del pagamento, le tue diciture — per la ristampa identica; si cancellano con la rata o con l'iscritto.

Dati del tuo account: nome dell'attività, città, email, telefono, stato di approvazione, piano, dati di fatturazione, versione delle condizioni accettata con data, ora, indirizzo IP e impronta dei documenti. Di questi dati siamo **titolari noi**, non responsabili: servono a gestire il contratto con te.

Natura e durata

Trattamento **continuativo**, per tutta la durata del servizio. Le durate di conservazione sono quelle del punto 10.

ALLEGATO II

Misure di sicurezza

Il contenuto del **punto 5** di questo accordo, compresa la sezione «Il rischio che resta», costituisce a tutti gli effetti l'allegato sulle misure tecniche e organizzative richiesto dall'art. 28, par. 3, lett. c, e dall'art. 32.

ALLEGATO III

Sub-responsabili autorizzati

FORNITORE	COSA FA	DOVE STANNO I DATI	NOTE
Supabase Pte. Ltd.	banca dati, autenticazione, archiviazione dei file	regione Francoforte , Germania	società di Singapore ; pubblica un proprio elenco di sub-fornitori
Cloudflare, Inc.	pubblicazione del pannello e del sito, esecuzione del nostro server (creazione degli accessi dei dipendenti, pagamenti del tuo piano, email di conferma), registrazione del dominio	rete globale; dal server passano le richieste, non vi restano archiviati dati degli iscritti	società statunitense
Plus Five Five, Inc. (Resend)	invio delle email di accesso, di servizio e della conferma di accettazione delle condizioni	infrastruttura di invio nella regione Irlanda ; trattamento principalmente negli Stati Uniti	società statunitense; tratta l'indirizzo email destinatario e il contenuto del messaggio
Google LLC	custodisce su Google Drive le copie di sicurezza cifrate, che contengono anche la tua rubrica	rete globale	società statunitense; riceve file cifrati con AES-256 di cui non ha la chiave. Nessun accordo sul trattamento : le copie stanno su un account Google personale (punto 6)

Lo strumento che copre il trasferimento fuori dall'Unione, per ciascun fornitore, è indicato al punto 12.

Riferimenti pubblici: Supabase — <https://supabase.com/legal/customer-resources/data-processing-addendum> · Resend — <https://resend.com/legal/dpa> e <https://resend.com/legal/subprocessors> · Cloudflare — <https://www.cloudflare.com/cloudflare-customer-dpa/> · Google — nessun accordo sul trattamento (punto 6); certificazione nel quadro UE-Stati Uniti su <https://www.dataprivacyframework.gov/list>

Non usiamo servizi di analisi statistica, di tracciamento né di pubblicità.

Stripe (Stripe Payments Europe, Ltd., Irlanda) gestisce **solo il pagamento del tuo piano**: riceve i tuoi dati di pagamento e di fatturazione, di cui siamo titolari noi. **Non riceve nessun dato dei tuoi iscritti**, e per questo non è un sub-responsabile di questo accordo: gli incassi che registri nel pannello per i tuoi iscritti sono annotazioni tue, non pagamenti che passano da noi o da Stripe.

I caratteri tipografici del pannello sono serviti dal nostro server: aprendo il pannello nessuna richiesta parte verso terzi.

ALLEGATO IV

Istruzioni di sicurezza per te

Queste sono misure che **spettano a te** come titolare, perché riguardano il computer e le persone della tua struttura, dove noi non arriviamo. Fanno parte dell'accordo: accettandolo ti impegni a seguirle.

Non lasciare il computer sbloccato. È la regola numero uno, perché il pannello mostra a schermo dati sanitari. Imposta il blocco automatico del sistema operativo dopo pochi minuti di inattività e prendi l'abitudine di bloccare a mano quando ti alzi, anche per un attimo.

Non tenere la postazione rivolta verso il pubblico. Lo schermo della reception è visibile da chi è in coda: gira il monitor, o tieni chiusa la pagina della rubrica quando non la stai usando.

Un accesso per ogni persona, mai credenziali condivise. Ogni dipendente ha il suo nome utente e la sua password, con i soli permessi che gli servono; il permesso «dati sanitari» dallo solo a chi ne ha bisogno per lavorare. Quando una persona lascia la struttura, disattiva o elimina subito il suo accesso. La casella email dell'account del titolare serve a recuperare la password: tienila protetta con una password forte e con la verifica in due passaggi.

Scarica una copia dei dati almeno una volta al mese dalla pagina Backup, e conservala in un posto sicuro: contiene dati personali e sanitari, quindi va protetta come il resto (non su una chiavetta lasciata in reception).

Esci dal pannello quando hai finito, e non salvare l'accesso su computer che non sono tuoi.

Consegna l'informativa e raccogli i consensi prima di inserire un iscritto, e in particolare i due consensi espliciti separati per il certificato medico e per le patologie, che questo servizio ti chiede prima di compilare quei campi. Il pannello non verifica che tu li abbia raccolti: è una responsabilità tua.

Scrivi nel campo patologie il minimo indispensabile, e solo se ti serve davvero per allenare quella persona in sicurezza. «Ernia lombare, evitare carichi sulla colonna» è quello che ti serve. Una diagnosi completa, il nome del medico o il racconto di una malattia non ti servono, e ti espongono.

Aggiorna la rubrica e cancella chi non frequenta più, entro i tempi del punto 10. Tenere dati che non servono più è una violazione dell'art. 5, e li tieni tu, non noi.

Avvisaci subito a info@ghisapro.com se sospetti che qualcuno sia entrato nel tuo account, se un computer con il pannello aperto è stato rubato, o se pensi che i dati siano finiti dove non dovevano.

Versione 2.2 — 6 ottobre 2026. Questo accordo si accetta insieme alle condizioni di servizio. Quando il testo cambia — per esempio per un sub-responsabile nuovo o per una misura di sicurezza diversa — il numero di versione cambia, te lo comunichiamo per email e ti viene chiesto di accettare la nuova versione.