INFORMATIVA PRIVACY, TRASPARENZA SULL'INTELLIGENZA ARTIFICIALE E QUADRO DEI CONSENSI

Omnia-X Health Professional S.B. S.r.l.
Codice fiscale e partita IVA 18288731005 — REA RM-1774703
Sede legale: Via delle Genziane 13E, 00012 Guidonia Montecelio (RM)
PEC: omniax@pec.omniaxhealthprofessional.com
Assistenza e richieste privacy: support@omniaxhealthprofessional.com

DOCUMENTO MASTER DI RIFERIMENTO. La presente versione individua Omnia-X Health Professional S.B. S.r.l. quale Titolare del trattamento, reca il contatto dedicato del Responsabile della protezione dei dati e identifica IMPLAN GROUP SRL quale Responsabile esterno direttamente designato per le attività tecniche affidate. La pubblicazione e l'operatività devono restare costantemente allineate all'architettura effettiva, ai fornitori e sub-responsabili realmente utilizzati, ai luoghi di trattamento, alle misure tecniche implementate e alla matrice di conservazione. Le clausole relative a funzioni future non autorizzano trattamenti oggi non determinati: ogni nuovo modulo, finalità o categoria di dati richiede una verifica preventiva e, quando necessario, una nuova informativa o un nuovo consenso.

PARTE I — INFORMATIVA PRIVACY GENERALE

Premessa e quadro normativo

La presente informativa descrive il trattamento dei dati personali effettuato tramite la piattaforma Omnia-X, le relative applicazioni, i portali professionali, le dashboard, i siti e gli altri ambienti digitali riconducibili a Omnia-X Health Professional S.B. S.r.l. Essa è redatta ai sensi degli articoli 12, 13 e 14 del Regolamento (UE) 2016/679 e deve essere letta insieme alle Condizioni Generali, alla Cookie Policy, agli eventuali accordi sul trattamento dei dati conclusi con Professionisti e Centri e alle informative contestuali visualizzate per specifici moduli. La Parte II (Quadro dei consensi e delle autorizzazioni) e la Parte III (Presidi interni obbligatori prima della pubblicazione) costituiscono parte integrante del presente documento.

Il sistema è progettato tenendo conto del Regolamento (UE) 2016/679, del decreto legislativo 30 giugno 2003, n. 196, come modificato, della direttiva 2002/58/CE e dell'articolo 122 del Codice privacy per cookie e strumenti di tracciamento, del Regolamento (UE) 2024/1689 sull'intelligenza artificiale, come modificato dal Regolamento (UE) 2026/1744, della legge 23 settembre 2025, n. 132, del Regolamento (UE) 2023/2854 sui dati, del Regolamento (UE) 2022/868 sulla governance dei dati e, per quanto progressivamente applicabile ai futuri servizi di dati sanitari elettronici, del Regolamento (UE) 2025/327 sullo Spazio europeo dei dati sanitari.

L'Artificial Intelligence Act è applicabile in via generale dal 2 agosto 2026, mentre le disposizioni relative ai sistemi ad alto rischio dell'Allegato III si applicheranno dal 2 dicembre 2027 e quelle relative ai sistemi ad alto rischio incorporati in prodotti regolamentati dell'Allegato I dal 2 agosto 2028. Omnia-X applicherà preventivamente a ogni nuovo modulo la classificazione del rischio, la verifica delle pratiche vietate, gli obblighi di trasparenza, la supervisione umana, la documentazione, la sicurezza, il monitoraggio e gli ulteriori adempimenti previsti dalla disciplina vigente al momento dell'attivazione.

Omnia-X ha adottato un Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001. La presente informativa costituisce parte del sistema integrato di compliance aziendale e si coordina con il Modello 231, il Codice Etico, le policy aziendali e i protocolli operativi applicabili, nel rispetto dell'autonomia e delle competenze proprie del Titolare, del Responsabile della protezione dei dati, delle funzioni di controllo e dell'Organismo di Vigilanza.

Articolo 1 — Titolare del trattamento

Il titolare del trattamento per le finalità determinate direttamente dalla piattaforma è Omnia-X Health Professional S.B. S.r.l., codice fiscale e partita IVA 18288731005, REA RM-1774703, con sede legale in Via delle Genziane 13E, 00012 Guidonia Montecelio (RM). Il Titolare può essere contattato mediante la PEC omniax@pec.omniaxhealthprofessional.com oppure mediante l'indirizzo support@omniaxhealthprofessional.com, indicando nell'oggetto "Richiesta privacy".

Articolo 2 — Responsabile della protezione dei dati

Omnia-X ha previsto la funzione di Responsabile della protezione dei dati (RPD/DPO) ai sensi degli articoli 37, 38 e 39 del GDPR. Il Responsabile formalmente designato opera con autonomia e indipendenza, è coinvolto tempestivamente nelle questioni riguardanti la protezione dei dati personali e costituisce punto di contatto per gli interessati e per l'Autorità di controllo. Il RPD/DPO è contattabile direttamente all'indirizzo e-mail dedicato dpo@omniaxhealthprofessional.com. Il nominativo del soggetto formalmente designato e i relativi dati sono comunicati al Garante secondo la procedura prevista dalla normativa applicabile.

Articolo 3 — Ambito dell'informativa e soggetti interessati

La presente informativa si applica agli utenti individuali, ai clienti che acquistano abbonamenti o componenti aggiuntivi, ai Professionisti e ai Centri che utilizzano le dashboard professionali, ai rappresentanti, amministratori e operatori autorizzati, ai soggetti che interagiscono con l'assistenza e alle persone i cui dati vengono legittimamente inseriti o importati nella piattaforma.

Quando un Professionista o un Centro tratta dati per finalità professionali proprie, comprese eventuali finalità di cura riservate a professionisti sanitari, esso può operare quale autonomo titolare del trattamento. Quando Omnia-

X tratta tali dati esclusivamente per conto del Professionista o del Centro e secondo istruzioni documentate, Omnia-X opera quale responsabile del trattamento ai sensi dell'articolo 28 del GDPR. Qualora le finalità e i mezzi siano determinati congiuntamente, i rispettivi ruoli saranno disciplinati mediante un accordo conforme all'articolo 26 del GDPR. La qualificazione dipende dalle attività concretamente svolte e non dalla sola denominazione contrattuale.

Articolo 4 — Categorie di dati trattati

Omnia-X può trattare dati identificativi e di contatto, credenziali, dati relativi all'età, al sesso biologico e alle informazioni necessarie alla personalizzazione del profilo, dati professionali, dati fiscali e di fatturazione, dati relativi all'abbonamento, al pagamento e alla gestione della relazione contrattuale.

La piattaforma può trattare dati relativi alla salute fisica o mentale, sintomi, anamnesi, patologie e condizioni dichiarate, referti, esami di laboratorio, parametri ematici, farmaci e integratori dichiarati, allergie, infortuni, limitazioni funzionali, dati sul sonno, recupero, stress, attività fisica, performance, nutrizione, idratazione, composizione corporea, ciclo mestruale, frequenza cardiaca, variabilità cardiaca, saturazione, temperatura, respirazione, misure antropometriche e ulteriori informazioni idonee a rivelare lo stato di salute.

La piattaforma può trattare dati genetici, varianti, referti genetici, predisposizioni e informazioni derivate da test genetici solo quando il relativo modulo sia attivato, l'importazione sia legittima e sia stato acquisito il consenso esplicito specificamente previsto. I dati biometrici sono trattati come categoria particolare solo quando utilizzati mediante tecniche specifiche per identificare in modo univoco una persona; le normali misure fisiologiche provenienti da wearable sono comunque trattate con le cautele previste per i dati relativi alla salute quando rivelano informazioni sullo stato fisico o mentale.

Sono inoltre trattati dati provenienti dai dispositivi e dalle integrazioni, identificativi tecnici, indirizzi IP, log di autenticazione, accessi e operazioni, dati di utilizzo, errori, ticket, comunicazioni, autorizzazioni, consensi, revoche, dati di sicurezza, indicatori di frode, nonché Output, score, correlazioni, protocolli proposti, trend, allerta e ulteriori dati derivati o inferiti dalla piattaforma.

Articolo 5 — Fonti dei dati

I dati possono essere forniti direttamente dall'Utente, inseriti da un Professionista o Centro legittimamente autorizzato, importati da Apple Health mediante HealthKit, da Health Connect, da wearable, sensori, applicazioni o altri servizi connessi, ricavati da documenti e referti caricati, ricevuti da partner tecnici autorizzati oppure generati dalla piattaforma attraverso calcoli, correlazioni, scoring, modelli statistici o sistemi di intelligenza artificiale.

Quando i dati non sono raccolti direttamente presso l'interessato, Omnia-X verifica che sussista un'idonea base giuridica e rende l'informativa prevista dall'articolo 14 del GDPR, salvo che ricorra una delle relative eccezioni. Il soggetto che inserisce dati di terzi deve essere legittimato a farlo e resta responsabile delle dichiarazioni e autorizzazioni di propria competenza.

Articolo 6 — Principi del trattamento

Omnia-X tratta i dati secondo i principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità, riservatezza e responsabilizzazione. Il Titolare è in grado di comprovare il rispetto di tali principi e mantiene la documentazione necessaria a dimostrare la conformità dei trattamenti. Le impostazioni predefinite devono limitare la raccolta, l'accesso e la condivisione a quanto necessario per la funzione selezionata. Le nuove funzionalità vengono sottoposte a valutazione privacy by design e by default prima dell'attivazione.

Articolo 7 — Creazione dell'account e gestione del rapporto contrattuale

I dati identificativi, di contatto, di autenticazione, contrattuali e amministrativi sono trattati per creare e gestire l'Account, autenticare l'Utente, attivare il Piano Base, gli Add-on e le Licenze B2B, consentire la fruizione dei servizi, gestire rinnovi, disdette, pagamenti, comunicazioni di servizio e assistenza. La base giuridica principale è l'esecuzione del contratto o di misure precontrattuali richieste dall'interessato ai sensi dell'articolo 6, paragrafo 1, lettera b), del GDPR. Per gli adempimenti connessi a obblighi normativi, fiscali, contabili o di identificazione, la base giuridica è l'articolo 6, paragrafo 1, lettera c), del GDPR. Per le attività strettamente necessarie alla sicurezza

dell'Account e alla prevenzione delle frodi, la base giuridica è il legittimo interesse ai sensi dell'articolo 6, paragrafo 1, lettera f), del GDPR, nel rispetto del bilanciamento con i diritti e le libertà dell'interessato.

La presa visione della presente informativa non costituisce consenso. Per i trattamenti necessari al contratto non viene richiesto un consenso revocabile, poiché l'eventuale rifiuto impedirebbe la creazione o gestione dell'Account.

Articolo 8 — Trattamento dei dati relativi alla salute per i servizi Omnia-X

Omnia-X tratta dati relativi alla salute per raccoglierli, organizzarli, correlarli, visualizzarli, conservarli nell'Account, produrre indicatori non diagnostici, consentire la consultazione dello storico e rendere disponibili le funzioni selezionate. Poiché tali attività tecnologiche non costituiscono, di per sé, diagnosi o terapia sanitaria svolta da Omnia-X, il trattamento delle categorie particolari effettuato direttamente dalla piattaforma, ivi incluso il trattamento mediante sistemi automatizzati, si fonda, di regola, sul consenso esplicito dell'interessato ai sensi dell'articolo 9, paragrafo 2, lettera a), del GDPR. Prima del conferimento del consenso, l'Utente è informato in modo chiaro circa le conseguenze della eventuale revoca, secondo quanto previsto dall'Articolo 38.

Il consenso deve essere libero, specifico, informato, inequivocabile, documentato e revocabile. L'Utente può utilizzare le sole funzioni che non richiedono dati relativi alla salute quando tecnicamente disponibili; la revoca del consenso può rendere impossibile mantenere attive le funzioni che necessitano di tali dati, senza incidere sulla liceità dei trattamenti eseguiti prima della revoca.

Articolo 9 — Dati genetici

I dati genetici sono trattati esclusivamente per le finalità chiaramente indicate nel modulo genetico attivato, quali importazione, organizzazione, rappresentazione e correlazione con altri dati dell'Utente, nel rispetto delle prescrizioni contenute nelle Autorizzazioni generali del Garante e delle disposizioni di cui all'articolo 2-septies del decreto legislativo 30 giugno 2003, n. 196, come modificato. L'attivazione richiede un consenso esplicito distinto rispetto al trattamento generale dei dati relativi alla salute. I dati genetici non sono utilizzati per finalità assicurative, creditizie, lavorative, di selezione, esclusione o discriminazione e non sono comunicati a datori di lavoro, assicurazioni, intermediari finanziari o soggetti analoghi.

L'utilizzo per ricerca, validazione scientifica o addestramento di modelli non è compreso nel consenso al servizio e richiede una base giuridica autonoma, garanzie ulteriori e, quando necessario, uno specifico consenso separato.

Articolo 10 — Dati biometrici e identificazione

Omnia-X non utilizza dati biometrici per identificare in modo univoco l'Utente salvo che venga attivata una funzione espressamente descritta e accompagnata da una specifica informativa e da un'idonea condizione di liceità. L'eventuale uso futuro di riconoscimento biometrico non sarà attivato mediante una generica accettazione della presente informativa.

Articolo 11 — Add-on IA

Quando l'Utente attiva l'Add-on IA, i dati disponibili nelle sezioni autorizzate possono essere analizzati mediante algoritmi e sistemi di intelligenza artificiale per generare correlazioni, riepiloghi, indicatori, priorità, suggerimenti e protocolli proposti. Il trattamento di dati relativi alla salute, genetici o di altre categorie particolari mediante tali sistemi si fonda sul consenso esplicito specifico per la funzione IA.

Gli Output sono strumenti informativi e di supporto, possono contenere errori e non costituiscono diagnosi, prescrizioni, prognosi cliniche, certificazioni o decisioni terapeutiche. L'Utente viene informato dell'interazione con sistemi di intelligenza artificiale e delle relative limitazioni. L'Utente ha il diritto di contestare gli Output generati e di richiedere una revisione umana mediante i canali indicati nell'Articolo 45. Omnia-X mantiene misure di supervisione umana, registrazione, verifica delle anomalie, sicurezza, gestione degli incidenti e aggiornamento della documentazione in funzione del ruolo assunto quale fornitore o deployer ai sensi dell'AI Act.

Articolo 12 — Add-on Predittivo e profilazione funzionale

L'Add-on Predittivo utilizza dati storici e correnti per produrre stime, scenari, probabilità e proiezioni sull'andamento di indicatori supportati. Tale attività costituisce profilazione quando utilizza trattamenti automatizzati per analizzare o prevedere aspetti relativi alla salute, alla performance, al comportamento o alle condizioni dell'Utente.

Il trattamento di dati appartenenti a categorie particolari per le funzioni predittive richiede un consenso esplicito separato. Le previsioni non rappresentano certezze e non sono utilizzate da Omnia-X per adottare decisioni esclusivamente automatizzate che producano effetti giuridici o analogamente significativi sull'Utente, salvo futura attivazione conforme all'articolo 22 del GDPR, accompagnata da informativa specifica, base giuridica idonea, diritto all'intervento umano, possibilità di esprimere la propria opinione e di contestare la decisione.

L'Utente può disattivare in qualsiasi momento le funzioni predittive e di profilazione funzionale dalle impostazioni dell'Account, senza che ciò pregiudichi l'accesso al Piano Base o alle ulteriori funzioni non dipendenti dall'Add-on Predittivo. La disattivazione interrompe le nuove elaborazioni predittive e la revoca del consenso è registrata secondo le modalità previste dalla Parte II.

Articolo 13 — Collegamento con Professionisti e Centri

L'Utente può autorizzare il collegamento del proprio Account a uno o più Professionisti o Centri. L'autorizzazione deve essere granulare, riferita a uno specifico destinatario, documentata e revocabile. La revoca interrompe i futuri accessi mediante la piattaforma, fatti salvi i trattamenti già lecitamente eseguiti e gli eventuali obblighi autonomi di conservazione del Professionista o Centro.

Omnia-X non presume che il pagamento della Licenza B2B da parte di un Professionista costituisca automaticamente autorizzazione all'accesso ai dati. Il sistema deve acquisire e registrare la scelta dell'Utente o una diversa base giuridica documentata. Ogni Professionista visualizza esclusivamente le categorie di dati e le funzioni corrispondenti ai permessi concessi.

Articolo 14 — Trattamenti per finalità di cura svolti da professionisti sanitari

Quando un professionista sanitario soggetto al segreto professionale tratta dati strettamente necessari per finalità di diagnosi, assistenza o terapia nell'ambito del rapporto con il paziente, il professionista opera di regola quale autonomo titolare e può fondare il trattamento sull'articolo 9, paragrafo 2, lettera h), e paragrafo 3, del GDPR, nonché sulla disciplina nazionale applicabile.

In tale scenario Omnia-X non acquisisce una propria finalità di cura e può operare quale responsabile del trattamento per l'hosting, la gestione tecnica e le altre attività svolte secondo le istruzioni del professionista, sulla base di un accordo conforme all'articolo 28 del GDPR. Il professionista resta responsabile dell'informativa sanitaria, delle basi giuridiche, della documentazione professionale e delle decisioni cliniche.

Articolo 15 — Professionisti non sanitari

Personal trainer, coach, preparatori atletici e altri professionisti non abilitati a svolgere attività sanitaria non possono utilizzare la base giuridica prevista per le finalità di cura riservate ai professionisti sanitari. Il loro accesso a dati relativi alla salute è subordinato alla scelta esplicita e informata dell'Utente, alle finalità professionali dichiarate, al principio di minimizzazione e ai limiti delle rispettive competenze.

Articolo 16 — Integrazioni con Apple Health, HealthKit, Health Connect e servizi terzi

Le integrazioni vengono attivate dall'Utente attraverso i sistemi di autorizzazione del dispositivo o del fornitore esterno. Omnia-X accede solo alle categorie selezionate e tecnicamente rese disponibili. L'Utente può revocare i permessi nelle impostazioni del dispositivo o del servizio; la revoca interrompe le future importazioni ma non determina automaticamente la cancellazione dei dati già acquisiti.

Apple, Google e gli altri fornitori trattano dati secondo proprie informative e in qualità determinate autonomamente. Omnia-X non controlla le modalità con cui tali soggetti raccolgono i dati prima della loro trasmissione. Prima dell'attivazione, l'Utente deve verificare le impostazioni e le informative dei servizi collegati.

Articolo 17 — Assistenza, ticket e comunicazioni di servizio

I dati contenuti nelle richieste di assistenza sono trattati per identificare l'Account, risolvere problemi, rispondere alle richieste, prevenire abusi, documentare le attività e migliorare la sicurezza del servizio. La base giuridica è l'esecuzione del contratto e, per le attività di sicurezza, il legittimo interesse di Omnia-X alla protezione della piattaforma, dei dati e dei propri diritti, nel rispetto del bilanciamento con i diritti e le libertà degli interessati.

L'Utente non deve inserire nei ticket informazioni sanitarie non necessarie. Le richieste di assistenza non costituiscono consulti medici e non sono utilizzate per formulare diagnosi o prescrizioni.

Articolo 18 — Sicurezza, prevenzione delle frodi e tutela della piattaforma

Omnia-X tratta log, indirizzi IP, identificativi di dispositivo, eventi di autenticazione, accessi, anomalie, operazioni, pagamenti e indicatori tecnici per proteggere Account e sistemi, prevenire frodi, abusi, accessi non autorizzati, manipolazioni di Output e revenue share, violazioni della proprietà intellettuale e incidenti informatici. La base giuridica è il legittimo interesse della Società e degli Utenti alla sicurezza, nel rispetto del bilanciamento con i diritti degli interessati.

Qualora una violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, Omnia-X comunica la violazione all'interessato senza ingiustificato ritardo, ai sensi dell'articolo 34 del GDPR, salvo che ricorra una delle condizioni di esenzione ivi previste. La comunicazione descrive la natura della violazione, le probabili conseguenze, le misure adottate o proposte e i recapiti del Responsabile della protezione dei dati.

Quando le attività di sicurezza coinvolgono categorie particolari di dati, il trattamento viene limitato a quanto strettamente necessario e si fonda sulla condizione di liceità applicabile, compreso l'accertamento, esercizio o difesa di un diritto in sede giudiziaria quando pertinente.

Articolo 19 — Pagamenti, fatturazione e adempimenti

I dati di pagamento possono essere trattati da prestatori specializzati che operano quali autonomi titolari o responsabili. Omnia-X tratta i dati necessari per autorizzare gli addebiti, gestire abbonamenti, rimborsi, storni, contestazioni, revenue share, fatturazione e obblighi contabili e fiscali. Le basi giuridiche sono l'esecuzione del contratto e l'adempimento di obblighi legali.

Articolo 20 — Comunicazioni operative

Omnia-X può inviare comunicazioni strettamente necessarie alla gestione dell'Account e del servizio, quali conferme, alert di sicurezza, modifiche contrattuali, scadenze, rinnovi, interruzioni, aggiornamenti e risposte ai ticket. Tali comunicazioni non richiedono consenso marketing quando sono necessarie all'esecuzione del contratto o all'adempimento di obblighi.

Articolo 21 — Marketing

L'invio di comunicazioni promozionali relative a prodotti, servizi, eventi o iniziative di Omnia-X mediante e-mail, SMS, messaggistica, notifiche promozionali o altri canali elettronici avviene sulla base di un consenso facoltativo e separato, salvo i casi espressamente consentiti dalla legge. Il mancato consenso non pregiudica l'accesso al servizio. Il consenso può essere revocato in ogni momento.

Omnia-X non vende né concede in locazione dati personali a inserzionisti e non utilizza dati relativi alla salute o genetici per pubblicità di terzi.

Omnia-X non cede, trasferisce, concede in licenza né rende altrimenti disponibili dati personali degli Utenti a soggetti terzi per finalità di profilazione creditizia, scoring assicurativo, selezione del personale, sorveglianza o qualsiasi altra finalità incompatibile con quelle indicate nella presente informativa.

Articolo 22 — Profilazione per finalità commerciali

L'eventuale analisi delle preferenze, dell'utilizzo della piattaforma o delle interazioni per personalizzare comunicazioni commerciali richiede un consenso distinto dal marketing generico. Tale profilazione non utilizza dati

relativi alla salute, genetici, referti, farmaci, patologie, Output sanitari o altre categorie particolari, salvo una futura finalità specifica che sia lecita, strettamente necessaria, separatamente descritta e accompagnata da un consenso esplicito autonomo. Omnia-X adotta come regola predefinita il divieto di utilizzare dati sanitari e genetici per targeting pubblicitario.

Articolo 23 — Ricerca, validazione e sviluppo scientifico

L'utilizzo di dati personali o pseudonimizzati per ricerca, validazione scientifica, studi osservazionali o sviluppo metodologico viene sottoposto a una valutazione separata delle finalità, delle basi giuridiche, delle garanzie, dell'eventuale necessità di autorizzazioni o pareri e dei diritti degli interessati. Il consenso prestato per l'erogazione del servizio non comprende automaticamente la ricerca.

Quando è possibile, Omnia-X utilizza dati anonimizzati. I dati realmente anonimizzati, non più riconducibili a una persona con mezzi ragionevolmente utilizzabili, non sono dati personali e possono essere conservati e utilizzati per finalità statistiche, di sicurezza, ricerca e miglioramento.

Articolo 24 — Addestramento, adattamento e valutazione dei modelli di intelligenza artificiale

Omnia-X non utilizza dati identificabili relativi alla salute, genetici o documenti sanitari per addestrare modelli generali o di terzi sulla base del solo consenso al servizio. L'eventuale utilizzo futuro per addestramento, fine-tuning, benchmarking o valutazione di modelli richiede una finalità specifica, una base giuridica autonoma, una valutazione d'impatto, misure di minimizzazione e, quando necessario, un consenso esplicito separato.

I contratti con fornitori di modelli devono vietare l'utilizzo dei dati Omnia-X per addestrare modelli propri del fornitore, salvo autorizzazione espressa e conforme alla presente informativa. I dati devono essere pseudonimizzati o minimizzati prima dell'invio quando tecnicamente possibile.

Articolo 25 — Adempimenti legali, controversie e tutela dei diritti

Omnia-X può trattare e conservare dati per adempiere a obblighi normativi, richieste delle autorità, ordini giudiziari, obblighi fiscali e contabili, nonché per accertare, esercitare o difendere diritti, gestire reclami, contestazioni, procedimenti, incidenti e violazioni. La conservazione per finalità difensive è limitata ai termini di prescrizione applicabili, salvo che un procedimento in corso ne richieda il prolungamento. Le basi giuridiche sono l'adempimento di obblighi legali, il legittimo interesse e, per le categorie particolari, l'articolo 9, paragrafo 2, lettera f), del GDPR quando applicabile e, ove ricorrano motivi di interesse pubblico rilevante, l'articolo 9, paragrafo 2, lettera g), del GDPR, nel rispetto delle condizioni e garanzie previste dalla normativa nazionale.

Articolo 26 — Assenza di decisioni esclusivamente automatizzate significative

Nella configurazione ordinaria, Omnia-X non adotta decisioni esclusivamente automatizzate che producano effetti giuridici o incidano in modo analogamente significativo sull'Utente. Score, alert, suggerimenti e previsioni supportano l'Utente o il Professionista e non determinano automaticamente accesso o esclusione da cure, assicurazioni, lavoro, credito, servizi essenziali o altri diritti.

Prima dell'eventuale attivazione di un trattamento rientrante nell'articolo 22 del GDPR, Omnia-X fornirà informazioni specifiche sulla logica utilizzata, sull'importanza e sulle conseguenze previste, attiverà le garanzie richieste e acquisirà la condizione di liceità necessaria.

Articolo 27 — Trasparenza e governance AI

Omnia-X informa l'Utente quando interagisce direttamente con un sistema di intelligenza artificiale o quando un contenuto è prodotto o trasformato automaticamente, nei casi previsti dall'AI Act. La piattaforma documenta la funzione del sistema, le categorie di dati utilizzate, le principali limitazioni, la supervisione umana, la gestione delle anomalie e i canali di contestazione.

I soggetti autorizzati all'utilizzo professionale delle funzioni IA devono ricevere formazione e istruzioni proporzionate al sistema impiegato. Omnia-X mantiene un inventario dei sistemi, dei modelli, delle versioni, dei fornitori e delle finalità e aggiorna la classificazione giuridica prima di ogni modifica sostanziale.

Eventuali Output anomali, contestati, incoerenti, inattesi o potenzialmente fuorvianti, l'impiego di dataset non autorizzati, la manipolazione di score, report o log e la diffusione di claim IA non approvati sono soggetti a monitoraggio, registrazione, gestione degli incidenti e procedure di escalation interne. Omnia-X può sospendere cautelativamente il modulo o l'Output interessato, preservare le evidenze, richiedere verifiche tecniche e umane e adottare misure correttive, senza che ciò comporti automaticamente il riconoscimento di un difetto generale del sistema.

Articolo 28 — Futuri sistemi ad alto rischio e moduli regolamentati

La presente informativa non costituisce autorizzazione preventiva all'attivazione di un sistema ad alto rischio o di un modulo qualificato come dispositivo medico. Prima di commercializzare o utilizzare una funzione che rientri nelle categorie ad alto rischio, Omnia-X dovrà completare la classificazione, la gestione del rischio, la governance dei dati, la documentazione tecnica, i log, la trasparenza, la supervisione umana, le verifiche di accuratezza, robustezza e cybersecurity, la valutazione d'impatto sui diritti fondamentali quando prevista, la registrazione e il monitoraggio successivo all'immissione sul mercato.

Qualora un modulo venga qualificato come dispositivo medico o software medicale, sarà disciplinato da documentazione, istruzioni, informativa privacy e condizioni specifiche coerenti con la normativa di settore. Nessuna qualificazione futura si estende automaticamente agli altri moduli.

Omnia-X non assume responsabilità per decisioni adottate dall'Utente o dal Professionista sulla base degli Output generati dalla piattaforma, ivi inclusi score, correlazioni, suggerimenti e protocolli proposti, che costituiscono esclusivamente strumenti informativi di supporto. L'Utente e il Professionista restano gli unici responsabili delle decisioni assunte sulla base di tali Output. Resta ferma la responsabilità di Omnia-X per dolo o colpa grave e per i danni derivanti dalla violazione degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati personali e di intelligenza artificiale.

Articolo 29 — Destinatari e comunicazione dei dati

I dati possono essere comunicati al Professionista o Centro selezionato dall'Utente, a dipendenti e collaboratori autorizzati di Omnia-X, a fornitori tecnici, cloud provider, software house, servizi di autenticazione, assistenza, pagamento, comunicazione e sicurezza, consulenti legali, fiscali e tecnici, autorità e soggetti ai quali la comunicazione sia necessaria per legge o per la tutela dei diritti. Tutti i destinatari sono vincolati da obblighi di riservatezza e sono tenuti a trattare i dati esclusivamente per le finalità per le quali la comunicazione è effettuata, nel rispetto delle istruzioni impartite e delle misure di sicurezza adeguate.

I dati relativi alla salute non sono diffusi. La comunicazione a terzi avviene soltanto sulla base di un idoneo presupposto giuridico, di una delega o autorizzazione dell'interessato o di un obbligo di legge. Quando la comunicazione comporta un trasferimento verso Paesi non appartenenti allo Spazio economico europeo, si applicano le garanzie previste dall'Articolo 31. L'elenco aggiornato delle categorie di destinatari e, quando opportuno, dei fornitori principali è reso disponibile su richiesta o in una sezione dedicata della piattaforma.

Articolo 30 — Responsabili e sub-responsabili del trattamento

I fornitori che trattano dati per conto di Omnia-X sono designati mediante accordi conformi all'articolo 28 del GDPR, con istruzioni documentate, obblighi di riservatezza, misure di sicurezza, assistenza nella gestione dei diritti e degli incidenti, regole sui sub-responsabili, restituzione o cancellazione dei dati e disponibilità delle informazioni necessarie agli audit. Omnia-X mantiene un elenco aggiornato dei responsabili e sub-responsabili del trattamento, indicante le funzioni svolte, i Paesi di trattamento e gli eventuali meccanismi di trasferimento, e lo rende disponibile agli interessati su richiesta o mediante la piattaforma.

Omnia-X resta Titolare del trattamento per le finalità determinate direttamente nell'ambito della Piattaforma. La designazione di IMPLAN GROUP SRL quale Responsabile esterno non trasferisce a quest'ultima la titolarità dei dati, non la autorizza a determinare finalità proprie e non consente utilizzi ulteriori, inclusi addestramento di modelli, profilazione, marketing, sfruttamento commerciale o comunicazione dei dati a terzi, salvo obblighi di legge o preventiva istruzione documentata di Omnia-X.

Per i fornitori che trattano dati personali o supportano funzioni critiche, inclusi software house, fornitori di modelli o servizi di intelligenza artificiale, cloud provider, soggetti di cybersecurity, autenticazione, pagamenti e assistenza, nonché consulenti privacy, fiscali, legali, compliance o bandi quando accedano a dati o sistemi rilevanti, Omnia-X applica controlli rafforzati di qualificazione, compliance, sicurezza, continuità operativa e governance. Tali controlli comprendono, in misura proporzionata al rischio, due diligence preventiva e periodica, verifica dei ruoli privacy, vincoli contrattuali, gestione dei subfornitori, trasferimenti, incidenti, audit, portabilità, restituzione o cancellazione dei dati e piani di uscita o sostituzione.

Alla data della presente informativa, il Responsabile esterno direttamente designato da Omnia-X ai sensi dell'articolo 28 del GDPR per le attività tecniche affidate è IMPLAN GROUP SRL, partita IVA e codice fiscale 07188110824, VAT IT07188110824, con sede in Via Nicolò Gallo 3, 90139 Palermo (PA), REA n. 442621, PEC implangroup@pec.it. IMPLAN GROUP SRL opera, nei limiti delle istruzioni documentate di Omnia-X, quale software house incaricata della gestione tecnica dei server e dell'infrastruttura applicativa e dei trattamenti strettamente necessari all'erogazione, manutenzione, sicurezza e continuità tecnica del servizio. Eventuali sub-responsabili utilizzati da IMPLAN GROUP SRL possono essere coinvolti esclusivamente nel rispetto dell'articolo 28 del GDPR e delle autorizzazioni previste dal relativo accordo; il relativo elenco aggiornato, insieme alle funzioni svolte, ai Paesi di trattamento e agli eventuali meccanismi di trasferimento, è mantenuto da Omnia-X ed è reso disponibile agli interessati con modalità adeguate o su richiesta.

Articolo 31 — Trasferimenti verso Paesi terzi

Omnia-X privilegia il trattamento nello Spazio economico europeo. Quando dati personali sono trasferiti verso Paesi non appartenenti allo Spazio economico europeo, il trasferimento avviene sulla base di una decisione di adeguatezza, delle clausole contrattuali standard della Commissione europea o di un altro strumento previsto dal Capo V del GDPR. In assenza di tali garanzie, il trasferimento può avvenire esclusivamente in presenza di una delle deroghe previste dall'articolo 49 del GDPR, nei limiti e alle condizioni ivi stabiliti. Omnia-X effettua, quando necessario, una valutazione dell'impatto del trasferimento e applica misure supplementari tecniche, contrattuali e organizzative.

L'Utente può chiedere informazioni sul meccanismo utilizzato e ottenere una copia delle garanzie applicabili, nei limiti necessari a proteggere segreti commerciali, sicurezza e diritti di terzi.

Articolo 32 — Tempi e criteri di conservazione

I dati necessari alla gestione dell'Account sono conservati per la durata del rapporto e, successivamente, per il periodo necessario a gestire richieste, obblighi e controversie. I dati contrattuali, fiscali e contabili sono conservati per il periodo previsto dalla legge e, di regola, per dieci anni dalla relativa registrazione.

I dati relativi alla salute, genetici e gli Output restano associati all'Account finché l'Utente mantiene attivo il servizio di storico, compresa l'eventuale modalità Archivio, oppure fino alla revoca del consenso o alla chiusura dell'Account, salvo che la conservazione sia necessaria per obblighi di legge o per la tutela di un diritto. Dopo la chiusura, la cancellazione dai sistemi attivi viene eseguita entro un periodo operativo non superiore a novanta giorni; le copie nei backup vengono sovrascritte secondo cicli tecnici che non superano centottanta giorni, salvo blocchi di conservazione documentati per obblighi normativi, procedimenti in corso o esigenze di tutela dei diritti.

I log di accesso ai dati sensibili e le evidenze di autorizzazione sono conservati, in via proposta, per cinque anni, salvo diversa necessità o termine stabilito dalla valutazione d'impatto. I log tecnici ordinari e di sicurezza sono conservati, in via proposta, per ventiquattro mesi, salvo incidenti o contenziosi. I ticket sono conservati per ventiquattro mesi dalla chiusura e più a lungo quando collegati a una controversia.

I consensi e le revoche sono documentati per tutta la durata del trattamento e per il periodo necessario a dimostrare la conformità. I dati per marketing sono conservati fino alla revoca e comunque sottoposti a revisione almeno ogni ventiquattro mesi; i dati di profilazione commerciale sono sottoposti a revisione almeno ogni dodici mesi. I dati anonimizzati possono essere conservati senza un termine predeterminato.

I tempi sopra indicati costituiscono una proposta legale prudenziale. Devono essere allineati ai cicli reali di database, backup, log, ticket, strumenti di pagamento e fornitori prima della pubblicazione.

Articolo 33 — Misure di sicurezza

Omnia-X adotta misure tecniche e organizzative adeguate al rischio, tenendo conto della natura dei dati, dello stato dell'arte, dei costi, delle finalità e della probabilità e gravità dei rischi. Le misure comprendono controllo degli accessi secondo necessità, autenticazione forte, cifratura in transito e a riposo per i dati appartenenti a categorie particolari, segregazione degli ambienti, pseudonimizzazione, registrazione degli accessi, backup, monitoraggio, gestione delle vulnerabilità, continuità operativa, procedure di incident response, formazione e impegni di riservatezza. Per le ulteriori categorie di dati, la cifratura a riposo è applicata ove tecnicamente possibile e proporzionata al rischio.

Nessuna misura garantisce sicurezza assoluta. Omnia-X verifica periodicamente l'efficacia dei presidi e aggiorna le misure in funzione dell'evoluzione dei rischi. Prima della pubblicazione, le misure indicate devono essere confermate sulla base dell'architettura effettiva e della documentazione della software house.

Articolo 34 — Valutazione d'impatto e consultazione preventiva

Le attività di scoring, profilazione e previsione su larga scala, il trattamento di dati relativi alla salute e genetici, l'integrazione di molteplici fonti e il monitoraggio sistematico possono comportare un rischio elevato per i diritti e le libertà. Omnia-X ha avviato e mantiene aggiornata una valutazione d'impatto sulla protezione dei dati, che deve essere completata prima dell'attivazione su larga scala di ciascun modulo interessato. Qualora il rischio residuo resti elevato nonostante le misure adottate, deve essere valutata la consultazione preventiva dell'Autorità di controllo ai sensi dell'articolo 36 del GDPR.

Gli esiti delle DPIA, delle valutazioni dei rischi privacy, AI e cyber e dei relativi piani di mitigazione possono essere utilizzati, in forma pertinente e proporzionata, anche ai fini dell'aggiornamento della mappatura dei rischi del Modello 231, dei protocolli aziendali e delle attività di vigilanza interna. Tale coordinamento non pregiudica l'indipendenza del Responsabile della protezione dei dati e non comporta la comunicazione all'Organismo di Vigilanza di dati personali o informazioni eccedenti rispetto alle finalità di controllo e prevenzione.

Articolo 35 — Minori

La piattaforma ordinaria è destinata a persone maggiorenni. Omnia-X non raccoglie consapevolmente dati di minori attraverso il normale flusso di registrazione. Qualora Omnia-X venga a conoscenza di aver raccolto dati personali di un minore in assenza dei presupposti di legge, provvede alla cancellazione tempestiva di tali dati e alla disattivazione dell'Account interessato, dandone comunicazione all'interessato o al soggetto esercente la responsabilità genitoriale ove possibile. L'eventuale attivazione futura di servizi per minori richiederà un percorso dedicato, verifica dell'età, identificazione del soggetto esercente la responsabilità genitoriale, informativa comprensibile e specifica valutazione delle basi giuridiche e dei rischi.

Articolo 36 — Conferimento dei dati

Il conferimento dei dati identificativi e contrattuali necessari alla creazione dell'Account è indispensabile per fornire il servizio. Il conferimento dei dati relativi alla salute, genetici, provenienti da dispositivi o necessari alle funzioni IA e predittive è facoltativo in senso giuridico, ma il rifiuto o la revoca impediscono l'utilizzo delle funzioni che dipendono da tali dati.

Il conferimento per marketing, profilazione commerciale, ricerca e addestramento dei modelli è sempre facoltativo e il rifiuto non incide sul Piano Base o sulle funzioni acquistate, salvo che la specifica attività costituisca un servizio distinto richiesto dall'Utente.

Articolo 37 — Diritti dell'interessato

L'interessato può chiedere conferma dell'esistenza dei dati, accesso, rettifica, integrazione, cancellazione, limitazione, opposizione, portabilità, informazioni sull'origine e sui destinatari e, nei casi previsti, informazioni significative sulla logica utilizzata nei trattamenti automatizzati. L'interessato ha altresì il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, e di

ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione, ai sensi dell'articolo 22 del GDPR. Può inoltre revocare i consensi senza pregiudicare la liceità del trattamento precedente.

I diritti possono essere esercitati mediante ticket, scrivendo a support@omniaxhealthprofessional.com o alla PEC omniax@pec.omniaxhealthprofessional.com. Omnia-X può chiedere informazioni ragionevoli per verificare l'identità e risponde nei termini previsti dal GDPR. Le richieste manifestamente infondate o eccessive possono essere gestite secondo l'articolo 12, paragrafo 5, del GDPR.

Articolo 38 — Revoca dei consensi e gestione delle conseguenze

La revoca deve essere semplice quanto il conferimento e può essere effettuata dalle impostazioni dell'Account o mediante richiesta. La revoca del consenso non pregiudica la liceità dei trattamenti eseguiti prima della revoca stessa. La revoca del consenso ai dati relativi alla salute determina la cessazione delle elaborazioni che richiedono tali dati e può comportare la disattivazione di Add-on o moduli. La revoca del consenso IA o predittivo impedisce nuove elaborazioni, mentre gli Output già generati sono cancellati o mantenuti secondo la scelta dell'Utente, gli obblighi applicabili e la matrice di conservazione.

La revoca dell'autorizzazione a un Professionista interrompe i futuri accessi mediante la piattaforma. Omnia-X informa il Professionista della revoca senza comunicare informazioni non necessarie.

Articolo 39 — Reclamo all'Autorità

L'interessato può proporre reclamo al Garante per la protezione dei dati personali o all'autorità di controllo competente nello Stato membro in cui risiede, lavora o si è verificata la presunta violazione. Resta salva la possibilità di ricorrere all'autorità giudiziaria.

Articolo 40 — Cookie e strumenti di tracciamento

Il sito e l'app possono utilizzare strumenti tecnici necessari al funzionamento e, solo previo consenso quando richiesto, strumenti analitici non assimilabili ai tecnici, di profilazione o di terze parti, nel rispetto delle Linee guida del Garante del 10 giugno 2021 in materia di cookie e altri strumenti di tracciamento. Informazioni dettagliate, durata, fornitori e modalità di scelta sono descritte in una Cookie Policy separata e gestite mediante un sistema di preferenze che consenta rifiuto, accettazione granulare e revoca.

Articolo 41 — Data Act, dispositivi connessi ed esportazione dei dati

Quando Omnia-X operi come fabbricante, fornitore di servizio correlato, titolare dei dati o destinatario ai sensi del Data Act, garantisce agli utenti l'accesso ai dati generati dall'uso del prodotto connesso o del servizio correlato e le ulteriori facoltà previste dalla disciplina, secondo modalità tecniche, contrattuali e informative specifiche. L'eventuale vendita o fornitura di wearable sarà accompagnata da condizioni e informativa separate.

Articolo 42 — Spazio europeo dei dati sanitari

Il Regolamento sullo Spazio europeo dei dati sanitari prevede un'applicazione progressiva, con importanti obblighi a partire dal 26 marzo 2029 e negli anni successivi. Omnia-X monitora gli atti di esecuzione e adegua interoperabilità, diritti di accesso, esportazione, logging e usi secondari prima che le relative disposizioni divengano applicabili ai propri servizi. La presente informativa non attribuisce oggi diritti o autorizzazioni non ancora applicabili.

Articolo 43 — Modello 231, segnalazioni e controlli interni

Omnia-X ha adottato un Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001. La presente informativa costituisce parte del sistema integrato di compliance aziendale e si coordina con il Modello 231, il Codice Etico, le policy aziendali e i protocolli operativi applicabili. Anomalie relative a dati, sicurezza, Output IA, dataset non autorizzati, score o report manipolati, claim IA non approvati, accessi, frodi e altre violazioni devono essere segnalate a Omnia-X mediante i canali operativi ufficiali. Omnia-X gestisce internamente la segnalazione attraverso le funzioni tecniche, legali, privacy, sicurezza e compliance e valuta autonomamente l'eventuale attivazione dei flussi previsti dal Modello 231 e l'interlocuzione con l'Organismo di Vigilanza.

Le segnalazioni operative, tecniche, privacy, di sicurezza o relative alla qualità degli Output devono essere indirizzate a Omnia-X e non direttamente all'Organismo di Vigilanza. Le segnalazioni che rientrano nell'ambito

materiale e soggettivo della normativa whistleblowing possono essere effettuate anche mediante il canale interno dedicato adottato dalla Società secondo il D.Lgs. 24/2023 e la relativa procedura. Il canale whistleblowing non sostituisce i normali canali di assistenza, data breach o incident management e deve essere utilizzato esclusivamente per le violazioni protette dalla normativa applicabile. Omnia-X assicura la separazione dei canali, la riservatezza e la gestione interna dei flussi verso le funzioni competenti e, quando previsto, verso l'Organismo di Vigilanza.

Articolo 44 — Modifiche dell'informativa

Omnia-X aggiorna la presente informativa quando cambiano finalità, categorie di dati, basi giuridiche, fornitori, trasferimenti, tempi di conservazione o funzionalità. Le modifiche sostanziali vengono comunicate con modalità proporzionate, inclusa la notifica individuale quando la modifica incida significativamente sui diritti dell'interessato. Le modifiche non sostanziali sono comunicate mediante pubblicazione sulla piattaforma. L'uso continuativo della piattaforma dopo la comunicazione di una modifica non costituisce consenso ai nuovi trattamenti che lo richiedono. Un nuovo trattamento incompatibile con le finalità originarie non viene fondato su un consenso generico già raccolto, ma richiede una nuova valutazione e, quando necessario, un nuovo consenso.

Articolo 45 — Contatti

Per informazioni, esercizio dei diritti, revoca dei consensi e segnalazioni privacy è possibile utilizzare il sistema interno di ticket, l'indirizzo support@omniaxhealthprofessional.com o la PEC omniax@pec.omniaxhealthprofessional.com. Il Responsabile della protezione dei dati (RPD/DPO) è contattabile direttamente all'indirizzo dedicato dpo@omniaxhealthprofessional.com. Le eventuali segnalazioni whistleblowing devono invece essere inoltrate mediante il canale dedicato indicato nella relativa procedura, quando la segnalazione rientra nell'ambito del D.Lgs. 24/2023.

PARTE II — QUADRO DEI CONSENSI E DELLE AUTORIZZAZIONI

Regole generali

L'accettazione delle Condizioni Generali e la presa visione dell'informativa privacy non sostituiscono i consensi. I consensi devono essere raccolti separatamente per finalità differenti, senza caselle preselezionate, mediante un atto positivo, e devono essere registrati con data, ora, versione dell'informativa, finalità, Account e canale di raccolta. La revoca deve essere disponibile nelle impostazioni con semplicità equivalente. I consensi eventualmente raccolti da soggetti minori di età non sono validi in assenza della verifica della responsabilità genitoriale e delle condizioni previste dall'articolo 8 del GDPR e dalla normativa nazionale applicabile.

Non è lecito ottenere oggi un consenso generico per qualsiasi utilizzo futuro dei dati o dell'intelligenza artificiale. Ogni funzione futura che modifichi sostanzialmente finalità, categorie di dati, destinatari, logica o conseguenze richiederà una nuova informazione e, quando necessario, un nuovo consenso.

Consenso A — Trattamento dei dati relativi alla salute per le funzioni Omnia-X

Testo breve destinato all'interfaccia: «Acconsento al trattamento dei miei dati relativi alla salute per utilizzare le funzioni Omnia-X selezionate, secondo l'Informativa Privacy.»

Descrizione estesa collegata: il consenso autorizza Omnia-X a raccogliere, organizzare, correlare, visualizzare e conservare i dati relativi alla salute inseriti o importati, nonché a produrre indicatori e Output non diagnostici necessari alle funzioni richieste. Il consenso non comprende marketing, ricerca, addestramento di modelli, comunicazione a Professionisti non selezionati, funzioni IA o predittive quando soggette a consenso separato.

Consenso B — Dati genetici

Testo breve destinato all'interfaccia: «Acconsento al trattamento dei miei dati genetici per il modulo genetico Omnia-X, secondo l'Informativa Privacy.»

Descrizione estesa collegata: il consenso autorizza esclusivamente importazione, organizzazione, visualizzazione e correlazione dei dati genetici per le funzioni selezionate. Non comprende utilizzo assicurativo, lavorativo, creditizio, pubblicitario, ricerca o addestramento di modelli.

Consenso C — Elaborazione mediante intelligenza artificiale

Testo breve destinato all'interfaccia: «Acconsento all'elaborazione dei dati autorizzati mediante le funzioni di intelligenza artificiale Omnia-X.»

Descrizione estesa collegata: il consenso permette l'uso delle categorie di dati selezionate per generare correlazioni, riepiloghi, indicatori, suggerimenti e protocolli proposti. Gli Output non sono diagnosi o prescrizioni e richiedono verifica umana. Il consenso può essere revocato senza disattivare il Piano Base.

Consenso D — Analisi predittiva e profilazione funzionale

Testo breve destinato all'interfaccia: «Acconsento alle analisi predittive e alla profilazione funzionale non decisionale previste dall'Add-on Predittivo.»

Descrizione estesa collegata: il consenso consente l'elaborazione automatizzata dei dati autorizzati per produrre stime, scenari e probabilità. Le elaborazioni non costituiscono diagnosi, prognosi cliniche o decisioni automatiche con effetti giuridici. La revoca interrompe le nuove analisi.

Autorizzazione E — Accesso del Professionista o Centro selezionato

Testo dinamico destinato all'interfaccia: «Autorizzo [NOME DEL PROFESSIONISTA/CENTRO] ad accedere alle categorie di dati da me selezionate attraverso Omnia-X.»

L'interfaccia deve mostrare il destinatario, il ruolo, le categorie di dati, le funzioni abilitate e la durata del collegamento. L'autorizzazione deve essere revocabile per singolo Professionista o Centro. Il pagamento della licenza da parte del Professionista non sostituisce questa scelta.

Autorizzazione F — Importazione da Apple Health, HealthKit, Health Connect o altri servizi

Testo destinato all'interfaccia: «Autorizzo Omnia-X a importare le categorie di dati selezionate dal servizio connesso.»

La selezione effettiva avviene anche nel sistema operativo o nel servizio di origine. L'Utente deve poter scegliere le singole categorie e revocare i permessi. La revoca interrompe le importazioni future.

Consenso G — Ricerca e validazione

Testo breve destinato all'interfaccia: «Acconsento all'utilizzo dei miei dati pseudonimizzati per gli specifici progetti di ricerca o validazione descritti.»

Il consenso deve essere associato a una scheda progetto che indichi finalità, responsabile, dati utilizzati, durata, destinatari, risultati attesi, rischi e modalità di revoca. Non deve essere raccolto in modo generico per ogni ricerca futura non determinata.

Consenso H — Addestramento o valutazione dei modelli

Testo breve destinato all'interfaccia: «Acconsento all'utilizzo dei miei dati pseudonimizzati per addestrare o valutare i modelli Omnia-X descritti nella scheda dedicata.»

Questo consenso è facoltativo, separato dalla fruizione del servizio e non può essere condizione per il Piano Base o per gli Add-on acquistati. La scheda deve descrivere dati, modello, scopo, durata, misure, destinatari e possibilità di revoca. L'utilizzo di dati genetici richiede un richiamo esplicito.

Consenso I — Marketing

Testo breve destinato all'interfaccia: «Acconsento a ricevere comunicazioni promozionali di Omnia-X tramite i canali selezionati.»

I canali devono essere selezionabili separatamente quando opportuno. Il consenso è facoltativo, revocabile e non comprende profilazione commerciale.

Consenso L — Profilazione commerciale

Testo breve destinato all'interfaccia: «Acconsento alla personalizzazione delle comunicazioni commerciali sulla base del mio utilizzo della piattaforma, esclusi i dati relativi alla salute e genetici.»

Il consenso è distinto dal marketing generico e non autorizza l'utilizzo di dati sanitari, genetici, farmaci, referti o Output per pubblicità.

Permessi e notifiche non qualificati come consenso privacy

Il permesso del sistema operativo per notifiche push, fotocamera, file, Bluetooth, sensori o localizzazione è gestito dal dispositivo e non sostituisce la base giuridica del trattamento. L'interfaccia deve spiegare perché il permesso è richiesto e permettere l'uso delle funzioni non dipendenti dal permesso.

PARTE III — PRESIDI INTERNI OBBLIGATORI PRIMA DELLA PUBBLICAZIONE

Articolo 1 — Mappatura dei trattamenti e ruoli

Devono essere mantenuti aggiornati il registro dei trattamenti, la mappa dei flussi, la classificazione dei dati, l'individuazione dei titolari, responsabili, contitolari e autonomi titolari, nonché gli accordi con Professionisti, Centri e fornitori. IMPLAN GROUP SRL deve essere formalmente designata quale Responsabile esterno mediante accordo ai sensi dell'articolo 28 del GDPR, coerente con le attività effettivamente affidate di gestione tecnica dei server e dell'infrastruttura applicativa. Devono essere identificati e riesaminati i fornitori critici e gli eventuali sub-responsabili, definendo per ciascuno responsabilità, dati accessibili, localizzazione, misure di sicurezza, continuità, audit, incidenti, trasferimenti e strategia di uscita.

Articolo 2 — Valutazione d'impatto

Deve essere completata una DPIA unica e modulare che copra dati sanitari e genetici, integrazione di fonti, scoring, profilazione, Add-on IA, Add-on Predittivo, accesso professionale, condivisione, conservazione dello storico, trasferimenti e incidenti. La DPIA deve essere aggiornata prima di ogni modifica sostanziale o nuovo modulo.

Articolo 3 — Responsabile della protezione dei dati

Il Responsabile della protezione dei dati deve essere formalmente designato con atto conforme agli articoli 37, 38 e 39 del GDPR, mantenuto coinvolto nelle valutazioni rilevanti e dotato di autonomia, accesso ai vertici e risorse adeguate. Il recapito dpo@omniaxhealthprofessional.com deve restare attivo, direttamente accessibile e presidiato dal Responsabile designato. La designazione e i dati di contatto del Responsabile della protezione dei dati devono essere comunicati al Garante per la protezione dei dati personali ai sensi dell'articolo 37, paragrafo 7, del GDPR. Ogni modifica del soggetto o dei relativi dati di contatto deve essere tempestivamente aggiornata nella Piattaforma, nell'informativa e nella comunicazione effettuata al Garante.

Articolo 4 — Consent management

Il sistema deve registrare consensi e revoche per finalità, versione, data, ora, Account, dispositivo e testo mostrato. Deve impedire l'attivazione di moduli che richiedono consenso in assenza di una manifestazione valida e propagare la revoca ai sistemi e fornitori coinvolti.

Articolo 5 — AI governance

Deve essere istituito un registro dei sistemi e modelli IA con ruolo Omnia-X, fornitore, versione, finalità, categorie di dati, base giuridica, rischio, test, limitazioni, supervisione, log, incidenti, fornitori, trasferimenti, sicurezza e data di riesame. Devono essere documentate formazione e istruzioni per personale e Professionisti autorizzati.

Articolo 6 — Contratti con fornitori IA

I contratti devono vietare il training del fornitore sui dati Omnia-X, limitare la conservazione, disciplinare subfornitori e trasferimenti, imporre sicurezza, notifica degli incidenti, cancellazione, audit e assistenza. Le chiamate ai modelli devono essere minimizzate e pseudonimizzate quando possibile.

Articolo 7 — Sicurezza e incident response

Devono essere documentati architettura, cifratura, ruoli, autenticazione, logging, backup, vulnerabilità, patching, segregazione, continuità, ripristino, test periodici e procedura di data breach. Professionisti e Centri devono segnalare gli incidenti operativi e privacy a Omnia-X, che gestisce gli eventuali flussi interni verso DPO, funzioni societarie, OdV e autorità. Deve inoltre essere mantenuto un canale whistleblowing separato, riservato alle segnalazioni che rientrano nell'ambito del D.Lgs. 24/2023 e gestito secondo la relativa procedura, senza confonderlo con assistenza e incident response.

Articolo 8 — Cookie e SDK

Deve essere svolto un audit di cookie, SDK, analytics, crash reporting, advertising identifier e tracking nell'app. Gli strumenti non necessari non devono essere attivati prima del consenso. La Cookie Policy deve riflettere tecnologie, fornitori e durate effettive.

Articolo 9 — Conservazione e cancellazione

La matrice di conservazione deve essere implementata tecnicamente su database, storage, log, ticket, backup e fornitori. La cancellazione deve essere propagata ai responsabili e documentata. L'Account Archivio deve essere una finalità reale e accessibile, non un espediente per conservare dati senza limite.

Articolo 10 — Diritti degli interessati

Devono essere predisposte procedure per accesso, rettifica, cancellazione, limitazione, opposizione, portabilità, revoca, autorizzazioni professionali e informazioni sull'IA. Le richieste devono essere tracciate e inoltrate ai responsabili coinvolti.

Articolo 11 — Minori

Finché non sarà progettato un percorso dedicato, il sistema deve impedire la registrazione ordinaria dei minori. L'eventuale apertura richiederà una DPIA aggiornata, verifica dell'età e responsabilità genitoriale, UX specifica e informative semplificate.

Articolo 12 — Data Act ed EHDS

Prima della vendita o concessione di wearable devono essere predisposte le informazioni Data Act sui dati generati, accesso, esportazione, condivisione e segreti commerciali. Prima delle scadenze EHDS applicabili devono essere verificati interoperabilità, formati, logging, diritti dell'utente, eventuale qualificazione come sistema EHR e condizioni per gli usi secondari.

Articolo 13 — Verifica finale

La pubblicazione deve avvenire solo dopo un confronto tra documento, interfacce, database, API, provider, contratti, consensi e comportamento reale del software. Qualsiasi promessa non corrispondente alla configurazione effettiva deve essere rimossa o corretta.

RIFERIMENTI NORMATIVI PRINCIPALI

Regolamento (UE) 2016/679; decreto legislativo 30 giugno 2003, n. 196, in particolare l'articolo 2-quinquies in materia di consenso del minore; direttiva 2002/58/CE; Linee guida del Garante del 10 giugno 2021 su cookie e strumenti di tracciamento; Linee guida EDPB 05/2020 sul consenso; Linee guida EDPB sulle decisioni automatizzate e profilazione; Linee guida EDPB 07/2020 sui concetti di titolare e responsabile; Linee guida EDPB WP 248 rev.01 sulla valutazione d'impatto sulla protezione dei dati; provvedimento del Garante n. 467 dell'11 ottobre 2018 sulle DPIA; Compendio del Garante del marzo 2024 sulle piattaforme che mettono in contatto pazienti e professionisti sanitari; Regolamento (UE) 2024/1689, come modificato dal Regolamento (UE) 2026/1744; legge 23 settembre 2025, n. 132; Regolamento (UE) 2023/2854; Regolamento (UE) 2022/868; Regolamento (UE) 2025/327; decreto legislativo 8 giugno 2001, n. 231; decreto legislativo 10 marzo 2023, n. 24; Linee Guida ANAC n. 1/2025 sui canali interni di segnalazione whistleblowing.