

Informativa Privacy

Informativa sul trattamento dei dati personali ai sensi degli artt. 13 e 14 del Regolamento (UE) 2016/679 e del D.lgs. 30 giugno 2003, n. 196

Versione 2.0 | Aggiornata al 28 luglio 2026 | In vigore dal: [●] | Sito triplete.org e applicazione Triplete

Stato del documento

Testo revisionato in forma professionale. Prima della pubblicazione devono essere completati i campi [●], verificati tutti i flussi reali e allineati contratti, SDK, fornitori, tempi di conservazione e trasferimenti internazionali.

La presente informativa descrive in modo trasparente come Empire S.r.l.s. unipersonale tratta i dati personali degli utenti che accedono al sito triplete.org, creano un account o utilizzano l'applicazione Triplete. Le informazioni sono organizzate per finalità, base giuridica, destinatari e tempi di conservazione.

1. Titolare del trattamento e contatti

Dato	Riferimento
Denominazione	Empire S.r.l.s. unipersonale (società con socio unico)
Sede legale	Via F. Ugoni 36 - Palazzo Skyline 18, 25126 Brescia (BS), Italia
P.IVA / Codice fiscale	03871350983
Registro delle Imprese / REA	Brescia - n. REA [●]
PEC	[●]
Email privacy	privacy@triplete.org
Responsabile della protezione dei dati (DPO)	Non nominato, salvo successivo aggiornamento / [● se nominato]

Il Titolare determina finalità e mezzi del trattamento. Le richieste relative ai dati personali possono essere inviate a privacy@triplete.org.

2. Ambito, categorie di interessati e provenienza dei dati

L'informativa riguarda gli utenti registrati, i visitatori del sito, i destinatari di comunicazioni, le persone invitate a leghe private e chi contatta l'assistenza. I dati sono raccolti direttamente dall'interessato, generati durante l'uso del servizio oppure ricevuti da fornitori tecnici strettamente necessari.

Quando un utente invita un'altra persona mediante email o numero di telefono, il dato è fornito dall'utente invitante. In questo caso Triplete tratta il dato esclusivamente per inoltrare l'invito e fornire all'interessato le informazioni richieste dall'art. 14 GDPR, nei limiti applicabili.

3. Dati personali trattati

Categoria	Esempi	Origine
Dati identificativi e di contatto	Nome, indirizzo email, numero di telefono, nickname, eventuale immagine profilo.	Forniti dall'utente.
Dati di autenticazione	Identificativi account e sessione, token, data e ora degli accessi, esito dell'autenticazione. Le credenziali sono gestite tramite il fornitore di autenticazione; Triplete non deve dichiarare di vedere o conservare la password in chiaro.	Generati dal servizio e dal fornitore di autenticazione.
Verifica telefonica	Numero di telefono, codice OTP o riferimento tecnico, data, ora, tentativi ed esito della	Utente e fornitore SMS.

TRIPLETE

	verifica.	
Dati di utilizzo e gioco	Pronostici/schedine, punteggi, classifiche, badge, leghe, ruolo nella lega, squadra del cuore, preferenze e impostazioni.	Generati durante l'uso.
Dati tecnici e di sicurezza	IP, dispositivo, sistema operativo, browser, lingua, versione app, log, eventi di sicurezza e identificativi tecnici.	Raccolti automaticamente.
Comunicazioni e assistenza	Contenuto dei messaggi, allegati, dati necessari a rispondere e storico della richiesta.	Forniti dall'utente.
Marketing e consensi	Canale scelto, data/ora, testo dell'informativa e della dichiarazione resa, revoca e prova del consenso.	Forniti dall'utente e registrati dal sistema.
Pagamenti e fatturazione - se attivi	Dati del piano, stato del pagamento, identificativo transazione, importi e dati fiscali. I dati completi della carta dovrebbero essere trattati dal provider di pagamento e non da Triplete.	Utente e provider di pagamento.
Dati relativi agli inviti	Email o telefono della persona invitata, mittente, lega, data ed esito dell'invito.	Forniti dall'utente invitante.
Notifiche e app	Token push, preferenze notifiche, eventi tecnici, crash e diagnostica, secondo gli SDK effettivamente installati.	Dispositivo, Apple/Google e SDK.

Dati particolari e contenuti liberi

Triplete non richiede dati appartenenti alle categorie particolari dell'art. 9 GDPR. Gli utenti non devono inserire informazioni sensibili in nickname, immagini, messaggi o altri campi liberi. Se tali dati vengono forniti spontaneamente e non sono necessari, potranno essere rimossi.

4. Finalità, basi giuridiche e conservazione

Finalità	Base giuridica	Dati principali	Conservazione prevista
Creazione e gestione dell'account; erogazione delle funzionalità Triplete.	Esecuzione del contratto - art. 6, par. 1, lett. b) GDPR.	Account, contatti, profilo, pronostici, classifiche, leghe, preferenze.	Per la durata dell'account. Dopo la chiusura: dati necessari per contestazioni fino a [24 mesi - confermare]; classifiche storiche rese anonime o pseudonimizzate secondo la scelta tecnica.
Autenticazione e verifica del numero di telefono.	Esecuzione del contratto e legittimo interesse alla sicurezza e unicità degli account - art. 6, par. 1, lett. b) e f).	Account, telefono, OTP/esito, log e tentativi.	Telefono per la durata dell'account; log OTP [12 mesi - verificare proporzionalità e provider].
Sicurezza, prevenzione frodi, bot, account multipli e abusi.	Legittimo interesse - art. 6, par. 1, lett. f); obblighi di sicurezza - artt. 5 e 32 GDPR.	IP, log, dispositivi, eventi, account e segnali di abuso.	Log ordinari [30-90 giorni - definire]; eventi accertati fino a [24 mesi] o per il tempo necessario alla difesa.
Calcolo dei punteggi e pubblicazione di classifiche, badge e risultati.	Esecuzione del contratto - art. 6, par. 1, lett. b).	Nickname, pronostici, punteggi, risultati e lega.	Per la durata del servizio/account; storico anonimo o con nickname secondo quanto definito nei Termini.
Invio di comunicazioni di servizio e notifiche operative.	Esecuzione del contratto - art. 6, par. 1, lett. b); legittimo interesse per avvisi di sicurezza.	Email, telefono, token push, preferenze.	Per la durata dell'account; log invio [12 mesi - verificare].
Marketing via email.	Consenso - art. 6, par. 1, lett. a) GDPR e art. 130 Codice Privacy.	Email, prova del consenso e interazioni strettamente necessarie alla gestione dell'invio.	Fino alla revoca o [24 mesi dall'ultima interazione - scegliere policy]. Prova del consenso e revoca per il termine necessario alla difesa, indicativamente fino a 5 anni.
Marketing via SMS o WhatsApp.	Consenso separato per canale - art. 6, par. 1, lett. a) e art. 130 Codice Privacy.	Telefono, canale, prova del consenso.	Come sopra; definire la regola effettiva.
Statistiche e miglioramento del servizio.	Legittimo interesse solo per misurazioni aggregate realmente assimilabili a strumenti tecnici; consenso per strumenti ulteriori.	Dati tecnici, pagine/eventi, IP anonimizzato secondo configurazione.	[● mesi] da confermare per ogni strumento.
Assistenza, reclami e richieste privacy.	Contratto, obbligo legale o legittimo interesse alla gestione e difesa.	Contatti, contenuto, allegati e log.	Assistenza [24 mesi]; richieste privacy e documentazione fino a [5

Pagamenti, abbonamenti e fatturazione - se attivi.	Contratto e obblighi legali - art. 6, par. 1, lett. b) e c).	Piano, pagamento, transazione, fattura e dati fiscali.	anni], salvo contenzioso. Documentazione contabile per 10 anni; dati operativi secondo contratto e contestazioni.
Accertamento, esercizio o difesa di diritti.	Legittimo interesse - art. 6, par. 1, lett. f); art. 9, par. 2, lett. f) solo ove eccezionalmente applicabile.	Dati pertinenti alla controversia.	Per la durata della controversia e dei termini di prescrizione/impugnazione.

Criterio di conservazione

I termini tra parentesi devono essere validati con i log reali e con le esigenze tecniche. Alla scadenza i dati devono essere cancellati o resi anonimi in modo irreversibile, salvo obblighi di legge o necessità di difesa.

5. Natura obbligatoria o facoltativa del conferimento

I dati necessari alla registrazione, all'autenticazione, alla verifica telefonica e all'erogazione delle funzioni richieste sono obbligatori: senza tali dati non è possibile creare o mantenere l'account o utilizzare le relative funzioni. I dati contrassegnati come facoltativi possono non essere forniti senza conseguenze sull'utilizzo ordinario del servizio.

I consensi marketing sono liberi, specifici e revocabili. Il rifiuto o la revoca non incidono sull'account, sui punteggi, sulle classifiche o sull'accesso alle funzioni non promozionali.

6. Soggetti autorizzati, responsabili e destinatari

I dati sono trattati da personale e collaboratori autorizzati, istruiti e vincolati alla riservatezza. Possono inoltre essere comunicati a fornitori che agiscono quali responsabili del trattamento ai sensi dell'art. 28 GDPR, oppure quali autonomi titolari per attività determinate dalla legge o dai rispettivi servizi.

Soggetto / categoria	Servizio	Ruolo privacy e localizzazione da verificare
[WUGIS - denominazione completa, sede e contatti]	Sviluppo, infrastruttura, database, manutenzione e motore di calcolo.	Definire ruolo, DPA, sub-responsabili e Paesi/server.
Clerk, Inc.	Account, autenticazione e gestione delle sessioni.	Responsabile del trattamento per i dati del cliente, secondo contratto/DPA; verificare configurazione, regioni, sub-responsabili e trasferimenti.
Infobip [entità contrattuale esatta]	Invio OTP via SMS.	Verificare entità, ruolo, DPA, Paesi di trattamento, sub-responsabili e retention.
Roxr Software Ltd / Clicky	Statistiche del sito, se effettivamente attivo.	Verificare ruolo, DPA, configurazione privacy, retention e trasferimenti.
[Fornitore email]	Email di servizio e marketing, se consentito.	Indicare entità, sede, ruolo, DPA, server e sub-responsabili.
Meta Platforms Ireland Ltd / servizio WhatsApp	Messaggi WhatsApp, solo ove attivati e consentiti.	Verificare prodotto utilizzato, ruoli, condizioni Business, destinatari e trasferimenti.
Apple e Google / relativi servizi	Distribuzione app, notifiche push, eventuali acquisti in-app, crash e servizi del dispositivo.	Ruolo può variare per singolo servizio; descrivere solo servizi realmente attivi.
[Provider pagamento]	Abbonamenti e pagamenti, se attivi.	Di regola autonomo titolare per alcuni trattamenti e responsabile per altri; verificare contratto.
[Crash reporting / logging / antifrode / supporto]	Diagnostica, sicurezza e assistenza.	Elencare ogni SDK/servizio effettivo.
Fornitori di dati sportivi, incluso API-Football [entità esatta]	Calendari, risultati, formazioni e statistiche sportive.	Confermare che non ricevano dati personali degli utenti; in caso contrario descrivere il flusso.
Consulenti e autorità	Assistenza legale, fiscale, contabile; adempimenti e richieste legittime.	Autonomi titolari o responsabili secondo l'attività.

Triplete non vende i dati personali e non li comunica a operatori di gioco o scommesse per loro autonome finalità commerciali. L'elenco aggiornato dei responsabili può essere richiesto a privacy@triplete.org.

7. Informazioni visibili agli altri utenti

Nelle classifiche e nelle leghe possono essere mostrati nickname, immagine profilo se scelta, punteggio, posizione, badge, squadra del cuore ed eventuali informazioni funzionali alla competizione. Nome, email, numero di telefono e credenziali non sono resi visibili agli altri utenti.

L'utente deve scegliere un nickname e un'immagine che non ledano diritti altrui e può utilizzare un nickname non identificativo. Le modalità di modifica e gli effetti sulla cronologia devono essere coerenti con i Termini e con la configurazione reale.

I dati delle persone invitate sono usati soltanto per recapitare e gestire l'invito. Se l'invito non viene accettato, il dato è cancellato entro [30 giorni - verificare]. L'utente invitante deve utilizzare recapiti che è legittimato a fornire.

8. Trasferimenti verso Paesi non appartenenti allo SEE

Alcuni fornitori o sub-responsabili possono trattare dati al di fuori dello Spazio Economico Europeo. In tali casi Triplete verifica l'esistenza di una decisione di adeguatezza oppure adotta garanzie appropriate, quali le Clausole Contrattuali Standard della Commissione europea, ed effettua le ulteriori valutazioni richieste sul contesto del trasferimento.

Per i fornitori statunitensi aderenti all'EU-U.S. Data Privacy Framework, il trasferimento può fondarsi sulla decisione di adeguatezza soltanto se l'entità destinataria e la categoria di dati risultano effettivamente coperte dalla certificazione in vigore. In alternativa o in via supplementare possono essere applicate le Clausole Contrattuali Standard.

Fornitore	Meccanismo da documentare prima della pubblicazione
Clerk, Inc.	Verificare adesione DPF in corso, DPA, eventuali SCC e lista sub-responsabili applicabile all'account Triplete.
Roxr Software Ltd / Clicky	[● verificare DPF, SCC o altro meccanismo; acquisire DPA e informazioni sui server].
Apple, Google, Meta, provider email/pagamenti/SDK	Verificare separatamente per entità e servizio; non usare formule generiche.

È possibile richiedere informazioni sulle garanzie adottate scrivendo a privacy@triplete.org, nei limiti in cui la divulgazione non comprometta segreti commerciali o misure di sicurezza.

9. Calcolo automatizzato di punteggi e classifiche

Triplete utilizza regole automatiche per confrontare pronostici e risultati sportivi e attribuire punteggi, badge e posizioni secondo il Regolamento di Gioco. La logica consiste nell'applicazione dei criteri predeterminati pubblicati nel Regolamento.

Tale calcolo non è destinato a produrre effetti giuridici sull'utente né effetti analogamente significativi ai sensi dell'art. 22 GDPR, in particolare ove non comporti premi, pagamenti, accesso al credito, esclusioni o conseguenze economiche. Eventuali sistemi antifrode che determinassero sospensioni automatiche dovranno essere descritti separatamente e accompagnati da garanzie adeguate, incluso l'intervento umano quando richiesto.

10. Età minima e dati dei minori

Triplete è destinato esclusivamente a utenti che abbiano compiuto 18 anni, secondo i Termini del servizio. Il Titolare non raccoglie intenzionalmente dati di minori. Se emerge che un account appartiene a un minore,

Triplete adotta le verifiche proporzionate necessarie e procede alla sospensione o cancellazione dell'account e dei dati non soggetti a obblighi di conservazione.

Un genitore o tutore può segnalare un possibile account di un minore scrivendo a privacy@triplete.org.

11. Misure di sicurezza e violazioni dei dati

Triplete adotta misure tecniche e organizzative adeguate al rischio, che possono comprendere cifratura delle comunicazioni, controllo degli accessi, segregazione degli ambienti, autenticazione rafforzata per gli amministratori, logging, backup, gestione delle vulnerabilità, aggiornamenti e procedure di risposta agli incidenti. Le misure effettive sono riesaminate periodicamente e non vengono descritte in modo tale da comprometterne l'efficacia.

In caso di violazione dei dati personali, il Titolare valuta il rischio e, quando previsto, notifica l'evento all'autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dalla conoscenza. Se la violazione può presentare un rischio elevato per i diritti e le libertà delle persone, gli interessati vengono informati senza ingiustificato ritardo, salvo le eccezioni previste dalla normativa.

12. Diritti dell'interessato

Nei casi previsti dal GDPR, l'interessato può esercitare i seguenti diritti:

- accesso ai dati e alle informazioni sul trattamento (art. 15);
- rettifica dei dati inesatti e integrazione di quelli incompleti (art. 16);
- cancellazione dei dati, quando ne ricorrono i presupposti (art. 17);
- limitazione del trattamento (art. 18);
- portabilità dei dati forniti, nei casi applicabili (art. 20);
- opposizione, per motivi connessi alla situazione particolare, ai trattamenti fondati sul legittimo interesse (art. 21);
- opposizione in qualsiasi momento al marketing diretto, senza necessità di motivazione;
- revoca del consenso in qualsiasi momento, senza pregiudicare la liceità del trattamento precedente alla revoca;
- diritto di non essere sottoposto a decisioni unicamente automatizzate nei casi previsti dall'art. 22.

Le richieste possono essere inviate a privacy@triplete.org. Prima di rispondere, Triplete può chiedere informazioni ragionevoli per verificare l'identità del richiedente. La risposta è fornita senza ingiustificato ritardo e, di regola, entro un mese; il termine può essere prorogato di due mesi nei casi previsti dall'art. 12 GDPR, informando l'interessato entro il primo mese.

L'esercizio dei diritti è gratuito, salvo richieste manifestamente infondate o eccessive. La cancellazione dell'account può essere disponibile anche nelle impostazioni dell'app; l'effettivo ambito della cancellazione resta soggetto agli obblighi di legge e ai dati necessari alla difesa.

L'interessato può proporre reclamo al Garante per la protezione dei dati personali o rivolgersi all'autorità giudiziaria. Le informazioni di contatto aggiornate del Garante sono disponibili sul sito istituzionale garanteprivacy.it.

13. Revoca dei consensi e comunicazioni promozionali

Il consenso può essere revocato con i sistemi resi disponibili in ciascun canale: link di disiscrizione nelle email, comandi indicati nei messaggi, impostazioni dell'account o richiesta a privacy@triplete.org. La revoca produce effetto per il futuro.

Le comunicazioni email non devono incorporare pixel o tecnologie di lettura/apertura ulteriori rispetto a quanto dichiarato. Qualora Triplete utilizzi misurazioni delle aperture, dei clic o del dispositivo, il relativo trattamento deve essere valutato separatamente e gestito in conformità alle regole applicabili, inclusa la disciplina del consenso ove richiesta.

14. Cookie, SDK e strumenti di tracciamento

Le informazioni dettagliate su cookie, SDK, identificatori e strumenti di misurazione sono riportate nella Cookie Policy disponibile su triplete.org/cookie-policy. La Cookie Policy e la presente informativa devono restare coerenti con la configurazione effettiva del sito e dell'app.

15. Aggiornamenti dell'informativa

Il Titolare può aggiornare la presente informativa in caso di modifiche normative, organizzative o tecniche. La nuova versione sarà pubblicata indicando la data di aggiornamento e di efficacia. Quando le modifiche incidono in modo significativo sui trattamenti o sulle aspettative ragionevoli degli utenti, Triplete fornirà un avviso adeguato e, se necessario, raccoglierà un nuovo consenso.

Riferimenti normativi essenziali

- Regolamento (UE) 2016/679, in particolare artt. 5, 6, 12-22, 25, 28, 32-34 e 44 e seguenti.
- D.lgs. 30 giugno 2003, n. 196, come modificato, in particolare artt. 122 e 130.
- Provvedimenti e linee guida del Garante applicabili ai trattamenti online, ai cookie e alle comunicazioni elettroniche.

Checklist riservata prima della pubblicazione

NON PUBBLICARE QUESTA PAGINA

Checklist operativa destinata al team legale, tecnico e amministrativo.

- ☐ Inserire data di efficacia, REA e PEC corretti; confermare eventuale DPO.
- ☐ Confermare campi obbligatori di registrazione e se nome, telefono e foto profilo sono realmente raccolti.
- ☐ Mappare tutti i flussi sito/app: pre-login, registrazione, OTP, gioco, leghe, inviti, notifiche, supporto, marketing, abbonamenti e cancellazione.
- ☐ Verificare chi conserva la password: con Clerk, evitare formule improprie come “la conserviamo cifrata”; descrivere il ruolo effettivo del provider.
- ☐ Definire retention reali e configurate per database, log, backup, OTP, assistenza, marketing, inviti, account cancellati e classifiche storiche.
- ☐ Completare denominazione e contratto WUGIS; definire titolare/responsabile, accessi, server, sub-responsabili e misure di sicurezza.
- ☐ Verificare entità contrattuale Infobip, DPA, retention OTP e Paesi coinvolti.
- ☐ Verificare Clicky: DPA, configurazione IP/cookie, retention, ruolo e trasferimenti.
- ☐ Elencare provider email, pagamenti, crash reporting, logging, supporto, antifrode, deep link e ogni SDK iOS/Android.
- ☐ Verificare Apple/Google/Meta per singolo servizio; evitare di attribuire un unico ruolo privacy a gruppi di servizi diversi.
- ☐ Confermare che API-Football e altri provider sportivi non ricevano identificativi, IP, user ID o telemetria degli utenti.
- ☐ Verificare certificazioni DPF dei destinatari USA alla data di pubblicazione e predisporre SCC/TIA quando necessario.
- ☐ Eseguire LIA documentata per sicurezza, prevenzione abusi, analytics tecnici e conservazione difensiva.
- ☐ Valutare DPIA se vengono introdotti monitoraggio sistematico, scoring antifrode invasivo, profilazione o trattamenti ad alto rischio.
- ☐ Verificare che l'eliminazione account sia realmente disponibile e definire esattamente cosa viene cancellato, anonimizzato o trattenuto.
- ☐ Verificare modalità di opposizione marketing e assenza/presenza di pixel nelle email; allineare moduli di consenso per canale.
- ☐ Allineare Informativa Privacy, Cookie Policy, Termini, Regolamento di Gioco, registro trattamenti, DPA, misure di sicurezza e app-store disclosures.
- ☐ Rimuovere tutti i campi [●], le note operative e questa checklist dalla versione pubblica.
- ☐ Ottenere validazione finale di un legale privacy sulla base dell'architettura e dei contratti realmente in uso.