

Conio Srl	Predisposta da: Funzione Compliance & Risk
	Versione di: Maggio 2026

Informativa Rischi

Termini e Condizioni - Direct

Allegato 2 – Termini e Condizioni Conio Direct

Con l'accettazione dei Termini e Condizioni, e l'utilizzo del Portafoglio per la custodia, l'acquisto, la vendita, lo scambio di Asset Digitali nonché il trasferimento di Bitcoin, il Cliente prende atto che la custodia di Asset Digitali, lo scambio di Asset Digitali con fondi o fra Asset Digitali nonché il servizio di collocamento degli stessi è caratterizzata da una natura altamente rischiosa in ragione di diversi fattori.

Occorre anche tenere in debita considerazione le rapide evoluzioni del contesto economico-giuridico di riferimento e geo-politico in generale, che possono incidere anche in maniera rilevante rispetto alle valutazioni svolte al momento dell'acquisto di Asset Digitali.

La presente informativa descrive i rischi associati all'utilizzo dei servizi su Asset Digitali offerti da Conio. Data la natura complessa e volatile di questi asset, è essenziale che Lei, in qualità di Cliente, comprenda appieno i rischi prima di operare. Il documento è diviso in due sezioni: la prima illustra i rischi generali, comuni a tutti i servizi; la seconda dettaglia i rischi specifici per ciascun servizio offerto. La lettura e la comprensione di questo documento sono un prerequisito indispensabile per l'utilizzo dei nostri servizi.

Rischi generali e comuni a tutti i servizi

Questi rischi sono intrinseci al mercato delle Asset Digitali e impattano, a diversi livelli, tutte le operazioni e i servizi da noi forniti.

- **Rischio di mercato (Volatilità):** Il valore degli Asset Digitali può subire fluttuazioni di prezzo estreme, rapide e imprevedibili. Tali fluttuazioni possono portare alla **perdita parziale o totale del capitale investito** in un breve lasso di tempo.
- **Rischio normativo:** Il quadro legale e fiscale relativo agli Asset Digitali è in costante e rapida evoluzione a livello globale. Futuri interventi normativi o decisioni da parte delle autorità potrebbero impattare significativamente l'operatività, il valore, la liquidità o la legalità di determinate Asset Digitali. Il MiCAR introduce per gli operatori obblighi e regole di condotta per la custodia degli euro e degli Asset Digitali, nonché obblighi di separazione patrimoniale tra le disponibilità degli operatori e dei clienti. Il Cliente che compra e detiene Asset Digitali non beneficia tuttavia delle garanzie e salvaguardie della disciplina di tutela dei depositanti;
- **Rischio tecnologico e di sicurezza della piattaforma:** Le operazioni si basano su tecnologie complesse (es. Distributed Ledger Technology). Nonostante la nostra azienda adotti i più elevati standard di sicurezza, esiste un rischio residuo di attacchi informatici sofisticati, bug software o malfunzionamenti che potrebbero compromettere la sicurezza e la disponibilità

degli asset custoditi. Una volta acquistati i Bitcoin, il proprietario riceve una chiave privata che ne determina il possesso. Tale chiave può essere rubata. Le chiavi private sono custodite con metodi vari e spesso sono detenute in portafogli virtuali, siano essi smartphone, computer o portatili. I meccanismi di protezione di questi portafogli virtuali consentono di custodire i propri Bitcoin, ma potrebbero non proteggere totalmente da hacker: le monete possono essere rubate, esattamente come dai portafogli reali. I furti e gli attacchi hacker possono impattare negativamente sulla reputazione del Bitcoin o del relativo mercato e, di conseguenza, influire negativamente sul prezzo di mercato di Bitcoin. I proprietari sono direttamente soggetti alla performance negativa e potrebbero perdere l'intero capitale.

- **Rischio legato alla sicurezza personale del cliente:** Lei è esposto a rischi che dipendono dalla sicurezza dei Suoi dispositivi personali (PC, smartphone). Attacchi di **phishing, malware o social engineering** mirati a Lei potrebbero portare al furto delle Sue credenziali di accesso e alla conseguente perdita dei Suoi asset. È Sua esclusiva responsabilità adottare adeguate misure di sicurezza personali (es. autenticazione a due fattori, password complesse, software antivirus).
- **Rischio di irreversibilità delle transazioni:** Le transazioni su blockchain sono, per loro natura, definitive e irreversibili. Un ordine eseguito o un trasferimento di Asset Digitali inviato a un indirizzo errato ("**fat-finger error**") non possono essere annullati o recuperati. È richiesta la massima attenzione da parte Sua nella gestione di ordini e indirizzi.
- **Rischio fiscale (Tax Risk):** Il trattamento fiscale delle plusvalenze e delle operazioni in Asset Digitali è complesso e soggetto a modifiche normative. È Sua esclusiva responsabilità informarsi sulla normativa fiscale vigente, dichiarare correttamente i Suoi asset e adempiere a tutti gli obblighi fiscali derivanti. La nostra azienda non fornisce consulenza fiscale.
- **Rischio AML/CFT (Antiriciclaggio e Contrasto al Finanziamento del Terrorismo):** In ottemperanza agli obblighi di legge, la nostra azienda monitora le transazioni per prevenire attività illecite. Qualora un'operazione o un account risultassero sospetti, potremmo essere obbligati per legge a **sospendere l'operatività, bloccare gli asset e segnalare l'attività alle Autorità competenti**, senza preavviso.
- **Assenza di schemi di garanzia:** A differenza dei depositi bancari, le Asset Digitali e i fondi detenuti **non sono coperti da alcun sistema di garanzia dei depositi** (es. FITD). Sebbene il Regolamento MiCAR imponga la segregazione patrimoniale tra gli asset dei clienti e quelli della società, in caso di nostra insolvenza il recupero dei Suoi asset potrebbe essere complesso, non immediato e non integralmente garantito.
- **51% attack:** se più del 50% dei computer, utilizzati in tutto il mondo per la verifica delle transazioni Bitcoin, fosse soggetto al controllo di un unico soggetto, ci sarebbe il rischio che un'unica parte controlli il 100% delle transazioni. Questo rischio, chiamato "51% attack", potrebbe causare il crollo di fiducia nel Bitcoin, comportando una sospensione degli scambi e conseguenti perdite per gli investitori, fino al rischio di totale perdita della somma investita.

Rischi specifici per servizio offerto

Di seguito sono dettagliati i rischi peculiari di ogni servizio che offriamo.

A. Servizio di scambio di crypto-attività con fondi (Valuta Fiat, es. Euro)

- **Rischio di liquidità:** Potrebbe riscontrare difficoltà nel convertire rapidamente le Sue Asset Digitali in Euro a un prezzo di mercato equo, specialmente per asset meno conosciuti o in fasi di alta turbolenza del mercato.
- **Rischio di controparte operativa:** Le operazioni di accredito e addebito in Euro coinvolgono circuiti bancari esterni. Eventuali ritardi, blocchi o fallimenti di questi intermediari potrebbero impattare la disponibilità dei Suoi fondi.
- **Rischio di delisting:** Potremmo decidere di cessare il supporto per una specifica Asset Digitali ("delisting") a causa di scarsa liquidità, problematiche tecnologiche o normative. In tal caso, esiste il rischio che il valore dell'asset crolli a seguito dell'annuncio.

B. Servizio di scambio di Asset Digitali con altre crypto-attività (crypto-to-crypto)

- **Rischio di volatilità relativa:** È esposto alla volatilità del prezzo tra le due Asset Digitali. È possibile che la Asset Digitali che acquista perda valore più velocemente di quella che ha venduto, risultando in una perdita.
- **Rischio dei protocolli sottostanti:** Scambiando asset consolidati con asset più nuovi o di nicchia ("altcoin"), si espone ai rischi specifici del protocollo di quest'ultimo (es. vulnerabilità del codice, scarsa adozione) che potrebbero portarne il valore a zero.
- **Rischio di delisting:** Similmente al punto A, una delle Asset Digitali della coppia di scambio potrebbe essere soggetta a delisting, impattando la Sua capacità di negoziarla.

C. Servizio di esecuzione di ordini per conto di clienti (collegato solo al servizio di collocamento)

- **Rischio di esecuzione (Slippage):** Il prezzo al quale il Suo ordine viene effettivamente eseguito potrebbe essere diverso (in senso peggiorativo) rispetto al prezzo visualizzato al momento dell'invio, specialmente in mercati molto volatili.
- **Rischio di mancata o parziale esecuzione:** In condizioni di mercato estreme, potrebbe non essere possibile eseguire il Suo ordine nella sua interezza al prezzo limite impostato, o potrebbe non essere eseguito affatto.
- **Rischio di delisting:** Se l'ordine riguarda una Asset Digitali in procinto di essere delistata, l'esecuzione potrebbe diventare impossibile o avvenire a condizioni di mercato sfavorevoli.

D. Servizio di collocamento di crypto-attività

- **Rischio di perdita totale del capitale:** Sta investendo in un progetto nuovo e altamente speculativo. Il fallimento del progetto è un'eventualità concreta che può portare alla **perdita completa e definitiva** del capitale investito.
- **Rischio di illiquidità a lungo termine:** Non vi è alcuna garanzia che si svilupperà un mercato secondario per l'asset acquistato. Potrebbe trovarsi nell'impossibilità di vendere il Suo investimento per un periodo indefinito.
- **Rischio legato alle informazioni (White Paper):** La Sua decisione si basa sul White Paper redatto dall'emittente. Sebbene soggetto a requisiti MiCAR, le informazioni potrebbero non riflettere pienamente i rischi tecnologici e di business del progetto.
- **Rischio di diluizione:** Future emissioni di token da parte del progetto potrebbero ridurre la Sua quota di partecipazione e avere un impatto negativo sul valore degli asset precedentemente collocati.

E. Servizio di custodia e amministrazione di Asset Digitali per conto di clienti

Quando usufruisce della custodia nella Sezione Asset i Suoi Asset Digitali per la custodia, si espone ai seguenti rischi specifici:

- **Rischio operativo e di sicurezza informatica (Furto):** Nonostante l'adozione di avanzate misure di sicurezza (come la conservazione della maggior parte degli asset in "cold storage" offline), esiste un rischio residuo di attacco informatico su larga scala che potrebbe superare le nostre difese, o di frode/errore umano da parte del nostro personale, portando al furto e alla perdita irreversibile dei Suoi asset.
- **Rischio di insolvenza del prestatore:** Ai sensi di MiCAR, i Suoi Asset Digitali sono segregate e legalmente separate dal patrimonio della nostra società. Tuttavia, in caso di nostra insolvenza, la procedura legale per la restituzione degli asset potrebbe essere complessa e richiedere tempo. Nonostante la protezione legale, non è possibile escludere a priori ritardi o costi legati al processo di recupero.
- **Rischio di gestione eventi di rete (Fork, Airdrop):** Le blockchain possono subire aggiornamenti significativi (fork) o distribuire nuovi token (airdrop). Conio non garantisce il supporto a ogni singolo fork o airdrop. Ciò potrebbe comportare la mancata ricezione di nuovi asset a cui Lei avrebbe altrimenti diritto, rappresentando una perdita di opportunità.
- **Rischio di commistione operativa**
Nel modello omnibus, le crypto-attività riferibili a più clienti possono essere detenute congiuntamente presso il medesimo wallet o conto, con conseguente esposizione a rischi di commistione operativa maggiori rispetto a una struttura integralmente segregata. Sebbene la Società mantenga registrazioni individuali delle posizioni, la gestione aggregata delle disponibilità può rendere più complessa la pronta ricostruzione delle spettanze individuali in caso di anomalie o eventi straordinari.

● **Rischio di errore o disallineamento contabile**

La corretta attribuzione delle cripto-attività al singolo Cliente, nei casi di custodia omnibus, dipende dal regolare funzionamento dei sistemi interni di registrazione, dal corretto flusso informativo con i sub-custodi e dall'efficacia dei processi di riconciliazione. Eventuali errori operativi, ritardi di aggiornamento, anomalie tecniche o incoerenze tra dati interni, evidenze on-chain e informazioni rese dai sub-custodi potrebbero incidere temporaneamente sulla corretta rappresentazione della posizione del Cliente.

● **Rischio relativo al sub-custode**

Qualora la custodia o sub-custodia sia affidata a soggetti terzi, il Cliente è esposto anche ai rischi connessi all'operatività, alla solidità e alla resilienza del sub-custode. Eventi quali insolvenza, malfunzionamenti tecnici, cyber incident, sospensioni operative, limitazioni ai prelievi o altre situazioni che interessino il sub-custode possono incidere sulla disponibilità, trasferibilità o tempestiva restituzione delle cripto-attività.

● **Rischio in caso di default o procedura concorsuale**

In caso di default, insolvenza o procedura concorsuale che coinvolga un sub-custode o altro soggetto rilevante della catena di custodia, la verifica delle spettanze individuali e la restituzione delle cripto-attività potrebbero richiedere tempi più lunghi e attività ricostruttive più complesse rispetto a una struttura di custodia pienamente segregata. Questo rischio è particolarmente rilevante nei modelli omnibus, nei quali la separazione delle posizioni dipende in misura significativa dalla qualità delle registrazioni e delle riconciliazioni disponibili.

● **Rischio di indisponibilità temporanea delle cripto-attività**

Anche in assenza di insolvenza, eventi operativi o tecnologici possono determinare indisponibilità temporanea delle cripto-attività o ritardi nell'esecuzione di istruzioni impartite dal Cliente. Tali eventi possono includere interruzioni dei sistemi, blocchi operativi, sospensioni tecniche, incidenti di sicurezza informatica, congestione di rete o verifiche straordinarie richieste dai fornitori di custodia o dalle autorità competenti.

● **Limiti di tutela del Cliente**

Le cripto-attività custodite non costituiscono depositi bancari e, salvo diversa previsione normativa applicabile, non beneficiano di sistemi di garanzia dei depositi o di analoghi meccanismi pubblici di protezione tipici del settore bancario. La tutela del Cliente dipende quindi, in misura rilevante, dall'effettività dei presidi di segregazione, dalla qualità delle registrazioni, dalla solidità della catena di custodia, dai controlli adottati e dalle misure di gestione dei rischi e degli incidenti.

F. Servizio di trasferimento di Asset Digitali per conto di clienti

- **Rischi Tecnologici e Operativi (Irrevocabilità ed Errori):** È il rischio più "tangibile" per l'utente che consiste nella possibilità di commissione di errori tecnologici derivanti da malfunzionamenti del sistema di gestione delle operazioni di trasferimento.

- **Irrevocabilità delle transazioni:** Una volta confermato, un trasferimento su blockchain non può essere annullato o stornato. Se il cliente invia fondi all'indirizzo sbagliato, i fondi sono persi per sempre.
- **Errori nell'indirizzo (Wallet Address):** Il rischio che il cliente digiti male l'indirizzo o selezioni la rete (network) sbagliata (es. inviare USDT su rete Ethereum a un indirizzo che supporta solo rete Tron).
- **Perdita delle credenziali/accessi:** Se il trasferimento avviene verso un wallet *non custodial* (self-hosted) di cui il cliente perde le chiavi private, il CASP non può recuperare i fondi.
- **Congestione della rete:** I tempi di conferma sulla blockchain non dipendono dal CASP ma dalla rete sottostante. In momenti di alto traffico, un trasferimento potrebbe restare "in pending" per ore o giorni.
- **Volatilità durante il trasferimento:** Poiché il valore delle crypto cambia rapidamente, il valore in euro ricevuto dal destinatario potrebbe essere diverso da quello inviato se trascorre tempo significativo prima della conferma.
- **Commissioni di rete (Gas Fees) variabili:** Il costo della transazione blockchain può aumentare improvvisamente, erodendo l'importo netto trasferito.
- **Travel Rule e Controlli AML:** Il CASP ha l'obbligo di verificare il beneficiario. Se l'indirizzo di destinazione risulta collegato ad attività illecite, sanzioni o "mixer", il CASP potrebbe dover bloccare o congelare il trasferimento per legge, impedendo al cliente di disporre dei propri asset.
- **Rifiuto della controparte:** un'altro prestatore di servizi di crypto-attività (il CASP del beneficiario) potrebbe rifiutare il deposito in arrivo se non riceve le informazioni corrette (Travel Rule), causando il rimbalzo dei fondi o il loro congelamento.
- **Attacchi Man-in-the-Middle o Malware:** Il rischio che il dispositivo del cliente sia infetto e modifichi l'indirizzo di destinazione al momento del "copia-incolla" (clipboard hijacking), facendo inviare i fondi a un hacker invece che al destinatario voluto.
- **Phishing:** Il rischio che il cliente stia inviando fondi a una truffa o a una finta piattaforma di negoziazione, credendo di operare legittimamente.

Disclosure sui presidi di mitigazione dei rischi inerenti la custodia su wallet omnibus e sulla sub-custodia

Titolarità dei beni del Cliente

Le cripto-attività e i fondi del Cliente sono e restano di proprietà esclusiva del Cliente anche quando siano trasferiti, depositati, registrati o comunque messi nella disponibilità di Conio ai fini della prestazione dei Servizi come riportato dall'art. 2.10. Tali beni non appartengono al patrimonio proprio di Conio e sono trattati secondo presidi organizzativi, contabili e contrattuali volti ad assicurarne la separazione rispetto alle risorse della Società.

Modelli di custodia adottati

La Società nella prestazione del servizio di custodia e amministrazione delle cripto-attività del Cliente utilizza modelli di custodia differenziati in funzione dell'asset, della rete DLT supportata, delle esigenze operative e dei presidi di sicurezza applicabili. In particolare, per talune cripto-attività la custodia può avvenire tramite wallet individuali multi-firma riconducibili al singolo Cliente; per altre cripto-attività la custodia può avvenire mediante un modello fiduciario che combina un sistema di allocazione individuale su ledger interno con la detenzione degli asset sottostanti presso wallet aggregati o wallet omnibus, anche detenuti presso sub-custodi terzi selezionati dalla Società ovvero rispettivamente:

- a. in modalità di custodia diretta, mediante wallet on-chain multi-firma, in cui il Cliente dispone di una delle chiavi private necessarie alla movimentazione; altresì
- b. in modalità di custodia tramite sub-custodi, mediante un sistema che combina registrazione individuale della posizione del Cliente su una DLT interna e detenzione aggregata degli asset sottostanti in wallet omnibus, dedicati esclusivamente alla detenzione di cripto-attività dei clienti Conio, senza commistione con asset di Conio, dei Sub-custodi o di altri clienti dei Sub-custodi.

Custodia diretta mediante wallet on-chain

Nei casi in cui Conio offra una soluzione di custodia diretta, le cripto-attività del Cliente sono detenute su wallet multi-firma on-chain associati al Cliente, secondo un'architettura tecnica che prevede la ripartizione delle chiavi tra soggetti distinti e l'utilizzo di controlli di sicurezza, inclusi meccanismi di autenticazione forte e procedure di recovery. In tale modello, la movimentazione delle cripto-attività richiede il rispetto delle regole tecniche e di autorizzazione previste dalla soluzione adottata da Conio per la specifica blockchain o cripto-attività supportata.

Wallet omnibus e allocazione individuale

Quando la custodia avviene tramite wallet omnibus, le cripto-attività di più clienti possono risultare aggregate on-chain in uno o più indirizzi o conti intestati o riferibili alla Società ma mai al sub-custode. In tali casi, la posizione individuale del Cliente è determinata e continuamente tracciata nei sistemi contabili e nei registri interni della Società, inclusi, ove applicabili, registri su infrastruttura DLT privata o sistemi equivalenti idonei ad assicurare l'attribuzione individuale, la tracciabilità delle movimentazioni e la riconciliazione con le consistenze aggregate detenute presso i wallet omnibus o i sub-custodi.

Quando le cripto-attività dei Clienti sono detenute in wallet omnibus, la segregazione patrimoniale è perseguita su più livelli.

- a. A livello interno, Conio mantiene evidenze e registrazioni atte a distinguere le posizioni dei Clienti dal patrimonio proprio della Società;
- b. A livello esterno, Conio privilegia l'utilizzo di infrastrutture o servizi di sub-custodia che consentano di segregare le posizioni riferibili a Conio da quelle del custode e degli altri clienti del medesimo custode.

Il Cliente prende atto che, nei modelli omnibus, la detenzione on-chain può avvenire in forma aggregata, mentre l'attribuzione individuale è assicurata mediante le risultanze del ledger interno e degli altri registri della Società.

Ricorso a sub-custodi

La Società può avvalersi di sub-custodi, depositari o altri fornitori terzi per la detenzione, gestione tecnica, messa in sicurezza o regolamento delle cripto-attività, in via ordinaria o eccezionale, inclusi scenari di continuità operativa, indisponibilità tecnica, manutenzioni o esigenze di esecuzione del servizio.

I sub-custodi sono selezionati secondo criteri di affidabilità, autorizzazione/regolamentazione, robustezza operativa, standard di sicurezza, livelli di segregazione offerti, coperture contrattuali, resilienza ICT e capacità di rendicontazione e riconciliazione.

La Società si avvale di sub-custodi esclusivamente quando delega ad altri la custodia e la gestione delle chiavi private dei wallet in cui custodisce le cripto-attività dei clienti.

Operatività ordinaria ed eccezionale

Il Cliente prende atto che, nell'operatività ordinaria, Conio privilegia soluzioni di custodia e sub-custodia idonee a rafforzare la segregazione e la resilienza del Servizio. In presenza di eventi eccezionali, manutenzioni, indisponibilità di partner primari, interruzioni API, incidenti operativi, esigenze di recovery o altri casi di business continuity, Conio può temporaneamente riallocare parte

delle cripto-attività o della relativa operatività verso soluzioni tecniche, wallet o fornitori alternativi, nella misura ragionevolmente necessaria a preservare la continuità, la sicurezza o il corretto regolamento dei Servizi.

Presidi organizzativi

La Società adotta presidi organizzativi volti a mitigare il rischio di custodia, inclusi, tra gli altri:

- a. segregazione dei compiti tra funzioni operative, tecnologiche, finanza e controllo; limitazione dei poteri dispositivi;
- b. workflow autorizzativi e tracciamento delle eccezioni;
- c. controlli di secondo livello da parte delle funzioni di controllo;
- d. audit periodici;
- e. monitoraggio dei fornitori terzi e riesame periodico delle relative performance, licenze, SLA e livelli di servizio.

Presidi contabili e di riconciliazione

La Società mantiene registrazioni/evidenze interne idonee a identificare in ogni momento, o comunque con la massima tempestività tecnicamente possibile, i diritti del Cliente sulle cripto-attività custodite. Sono effettuati periodicamente controlli di riconciliazione tra:

- a. posizioni individuali del Cliente risultanti dai sistemi interni;
- b. saldi aggregati delle posizioni individuali dei Clienti;
- c. evidenze dei saldi del wallet omnibus fornite dai sub-custodi;
- d. dati disponibili sulle blockchain pubbliche, ove accessibili e pertinenti.

Eventuali anomalie o disallineamenti sono sottoposti a procedure di escalation, verifica e rimedio secondo le procedure interne della Società.

Presidi ICT e di sicurezza

La Società adotta presidi ICT proporzionati ai rischi di custodia, inclusi, a titolo esemplificativo:

- a. architetture a segregazione logica e per ambienti;
- b. cifratura dei dati in transito e a riposo;
- c. gestione e rotazione delle chiavi crittografiche;
- d. autenticazione forte e multi-fattore;
- e. controlli su dispositivi e accessi, logging, monitoraggio di sicurezza, SIEM, EDR/XDR, IDS, procedure di patching e vulnerability management, protezioni API/WAF;
- f. procedure di incident response, business continuity e disaster recovery.

- g. Per i modelli multi-firma o equivalenti, la Società adotta inoltre meccanismi di approvazione a più fattori o a più parti, in modo da ridurre il rischio di firma non autorizzata o di compromissione di una singola chiave.

Per i modelli multi-firma o equivalenti, la Società adotta inoltre meccanismi di approvazione a più fattori o a più parti, in modo da ridurre il rischio di firma non autorizzata o di compromissione di una singola chiave.