

Informativa sulla Policy di custodia e amministrazione delle Cripto-attività

La presente Informativa deve essere letta congiuntamente ai Termini di Servizio e alle altre Informative applicabili; in caso di discrepanze, prevalgono i Termini di Servizio. CheckSig può aggiornare la presente Informativa per riflettere evoluzioni normative, tecnologiche o operative dei Servizi dandone comunicazione al Cliente secondo quanto previsto dai Termini di Servizio.

1 Premessa

1. I termini con iniziale maiuscola non definiti nella presente Informativa hanno il significato attribuito nei Termini di Servizio.
2. La presente Informativa descrive in modo specifico le caratteristiche, le modalità di prestazione, i presidi di sicurezza e i principali rischi del servizio di custodia e amministrazione di cripto-attività prestato da CheckSig.
3. Il Cliente può in ogni momento richiedere via e-mail una copia digitale della Policy di custodia e amministrazione delle Cripto-attività.

2 Principi generali nella tutela delle Cripto-attività dei Clienti

1. I prestatori di servizi per le Cripto-attività che offrono servizi di custodia e amministrazione per conto dei Clienti sono tenuti a separare le Cripto-attività detenute per conto dei Clienti dal proprio patrimonio e a garantire che i mezzi di accesso alle Cripto-attività dei Clienti siano chiaramente identificati come tali.
2. La Custodia riguarda esclusivamente la conservazione e l'amministrazione delle Cripto-attività, senza alcuna garanzia circa il valore, la stabilità o il funzionamento delle tecnologie sottostanti.
3. In conformità alla normativa applicabile e ai Termini di Servizio:
 - a. le Cripto-attività detenute in custodia sono giuridicamente, contabilmente e operativamente separate dal patrimonio di CheckSig e sono detenute nell'interesse dei Clienti;
 - b. i creditori di CheckSig non vantano diritti di rivalsa sulle Cripto-attività dei Clienti nei limiti e secondo le modalità previste dalla normativa applicabile e dalle misure di opponibilità adottate dalla Società;
 - c. la proprietà delle Cripto-attività e dei fondi *fiat* resta sempre in capo ai Clienti, anche quando tali disponibilità sono trasferite a CheckSig per la fruizione dei Servizi;
 - d. CheckSig non utilizza, investe o impiega le Cripto-attività o i fondi dei Clienti per finalità diverse dall'erogazione dei Servizi richiesti.
4. La tutela delle Cripto-attività comprende altresì:

- a. la disponibilità di sistemi e procedure che consentono ai Clienti di esercitare i diritti connessi alle Cripto-attività, anche in occasione di eventi o operazioni che richiedano una risposta o scelta del Cliente;
 - b. la predisposizione di presidi che assicurano l'identificazione delle Cripto-attività e dei mezzi di accesso - come riferibili alla custodia per conto Clienti;
 - c. la presenza di sistemi e procedure che assicurano la restituzione delle Cripto-attività ai Clienti e la continuità operativa nella gestione dei mezzi di accesso, secondo quanto previsto dai Termini di Servizio, dalla presente Informativa e dalla normativa applicabile.
5. Le Cripto-attività in Custodia non beneficiano di garanzie pubbliche di rimborso né di tutele assimilabili ai sistemi di garanzia dei depositi bancari o degli investitori. Le eventuali coperture assicurative private operano nei limiti, alle condizioni e secondo i massimali previsti dalle relative polizze e non costituiscono garanzia assoluta di integrale ristoro in ogni circostanza.

3 Presidi di tutela delle Cripto-attività dei Clienti

A tutela delle Cripto-attività dei Clienti, CheckSig adotta presidi articolati su più livelli, idonei a garantire separatezza, identificazione, esercizio dei diritti connessi, riconciliazione, controllabilità e restituzione delle Cripto-attività nel rispetto delle istruzioni del Cliente e della normativa applicabile.

1. Presidi contrattuali

I Termini di Servizio stabiliscono espressamente che la proprietà delle Cripto-attività e dei fondi fiat resta in capo ai Clienti. Analogamente, le prassi operative e gli accordi con fornitori, CASP e istituti bancari prevedono misure coerenti con la tutela e la segregazione delle disponibilità dei Clienti, nei limiti consentiti dalla controparte e dalla normativa applicabile.

I Termini di Servizio e le Informative applicabili disciplinano inoltre:

- a. le modalità di prestazione del servizio di custodia e amministrazione e i relativi limiti;
- b. le modalità con cui il Cliente può impartire istruzioni, ricevere comunicazioni e ottenere la rendicontazione periodica;
- c. i presidi di segregazione e tutela, incluse le misure di opponibilità verso terzi;
- d. le condizioni di gestione di eventi straordinari, incluse, ove applicabili, quelle relative a fork.

2. Presidi organizzativi e contabili

CheckSig mantiene evidenze contabili interne idonee a ricostruire in modo puntuale, aggiornato e verificabile la posizione di ciascun Cliente, distinguendo in modo chiaro le Cripto-attività e i fondi fiat detenuti per conto della clientela da quelli della Società. Nell'ambito del modello operativo di custodia adottato dalla Società, le Cripto-attività della clientela sono detenute secondo un modello di custodia di tipo omnibus, nel quale le disponibilità aggregate sono custodite in wallet di custodia controllati da

CheckSig. In tale configurazione la titolarità individuale delle Cripto-attività è mantenuta attraverso registrazioni contabili interne dedicate a ciascun Cliente, distinte dalle evidenze relative al patrimonio proprio della Società.

Il sistema contabile interno consente di associare in modo univoco a ciascun Cliente le relative disponibilità e movimentazioni, garantendo la piena tracciabilità e ricostruibilità delle posizioni individuali e la coerenza tra i saldi complessivi detenuti nei wallet di custodia e le evidenze contabili interne.

Tale assetto consente alla Società di identificare e in ogni momento le disponibilità riferibili a ciascun Cliente ai fini della rendicontazione alla clientela, delle attività di riconciliazione e dell'esecuzione delle istruzioni impartite dal Cliente in relazione restituzione delle Cripto-attività, nel rispetto della normativa applicabile.

A tal fine:

- a. CheckSig utilizza un registro interno delle posizioni (CheckSig-DB) che associa univocamente a ciascun Cliente le disponibilità in Cripto-attività e, ove applicabile, in fondi fiat, e registra le relative movimentazioni e gli eventi rilevanti;
- b. le evidenze contabili sono aggiornate in via continuativa;
- c. le evidenze contabili sono oggetto di riconciliazione con cadenza almeno giornaliera tra i saldi individuali registrati nei sistemi informativi interni e le disponibilità aggregate detenute nei wallet di custodia e/o presso eventuali accounts "CASP c/Terzi", secondo le procedure interne e in funzione delle caratteristiche operative dei sistemi adottati dalla Società;
- d. la rendicontazione periodica resa disponibile al Cliente consente la verifica delle posizioni e delle relative movimentazioni, includendo, ove disponibili, anche i dati tecnici delle operazioni (quali, ad esempio, gli identificativi delle transazioni on-chain).

Tali presidi concorrono, inoltre, a garantire:

- a. l'identificazione delle Cripto-attività detenute per conto della clientela;
- b. la ricostruibilità in ogni momento della posizione individuale di ciascun Cliente;
- c. la possibilità di restituzione delle stesse secondo le istruzioni del Cliente e le procedure previste.

3. Presidi tecnologici

CheckSig adotta misure idonee a proteggere i mezzi di accesso crittografici associati alle Cripto-attività detenute per conto dei Clienti, incluse misure di crittografia, autenticazione a più fattori, segregazione degli accessi, logging, tracciabilità delle operazioni e conservazione dei dispositivi di sicurezza hardware (HSM) in cassette di sicurezza, al fine di prevenire accessi non autorizzati e ridurre i rischi informatici.

La gestione dei wallet e delle movimentazioni avviene secondo logiche di autorizzazione collaborativa (Multi-Signature o Multi-Party Computation) e segregazione dei ruoli, con l'obiettivo di:

- a. vincolare le movimentazioni alle sole istruzioni valide e alle procedure autorizzative predefinite;

- b. garantire la restituzione delle Cripto-attività ai Clienti mediante processi controllati di prelievo e trasferimento;
 - c. garantire l'identificazione dei mezzi di accesso come riferibili alla custodia per conto Clienti.
4. **Presidi di continuità operativa, ripristino e restituzione**
- CheckSig adotta presidi di business continuity e disaster recovery, incluse procedure e dispositivi dedicati, volti ad assicurare la continuità operativa nella custodia e amministrazione e, in particolare, la capacità di movimentare e restituire le Cripto-attività ai Clienti anche in scenari di indisponibilità parziale di dispositivi, infrastrutture o soggetti approvanti, secondo le procedure interne e i vincoli tecnici del protocollo sottostante.
- In caso di incidente che possa incidere sulla disponibilità, integrità o sicurezza delle Cripto-attività detenute in custodia, CheckSig attiva procedure di emergenza volte alla protezione dei fondi e alla continuità operativa, nonché, ove applicabile, alla comunicazione al Cliente e alle Autorità competenti nei termini previsti dalla normativa e dalla documentazione contrattuale.
5. **Presidi assicurativi**
- CheckSig integra i presidi contrattuali, organizzativi e tecnologici con coperture assicurative private contro il furto delle Cripto-attività depositate presso la Società e altri rischi connessi alla custodia, nei limiti e secondo le condizioni della polizza.
- Le coperture assicurative:
- a. non sostituiscono né limitano i presidi di segregazione patrimoniale e di sicurezza adottati dalla Società;
 - b. non costituiscono garanzia pubblica o legale;
 - c. non costituiscono garanzia assoluta di integrale ristoro in ogni circostanza;
 - d. operano esclusivamente nei casi e secondo le modalità previste dalle condizioni di polizza applicabili.

4 Utilizzi complementari della Custodia

Fermo quanto previsto dai Termini di Servizio e dalle specifiche Informative applicabili, la Custodia può essere utilizzata per ottenere benefici complementari.

1. **Custodia con Staking protocollare**
- a. Il Servizio di Custodia con Staking protocollare è attivato esclusivamente su istruzione e richiesta del Cliente.
 - b. L'attivazione dello Staking può comportare periodi di indisponibilità temporanea delle Cripto-attività oggetto di vincolo, in funzione delle regole del protocollo sottostante e delle relative tempistiche tecniche, inclusi eventuali periodi di attivazione, disattivazione o "timelock".
 - c. Lo Staking può comportare rischi specifici connessi al funzionamento del protocollo, quali, a titolo esemplificativo, penalità o meccanismi di "slashing" in caso di malfunzionamenti o violazioni delle regole di rete. CheckSig adotta presidi tecnici e organizzativi volti a minimizzare tali rischi, fermo restando

che nella misura in cui dipendono dal protocollo sottostante non sono integralmente eliminabili.

- d. I tempi tecnici di attivazione e disattivazione dipendono dal protocollo sottostante, dalle condizioni di rete e, ove previsto, dall'eventuale coda di attesa per l'ingresso o l'uscita dallo staking. CheckSig rende disponibili in Area Privata stime aggiornate sui tempi tecnici previsti. A fini meramente esemplificativi, i tempi attesi possono essere, a seconda dell'asset e delle condizioni di rete:
 - i. per Ethereum (ETH), nell'ordine di giorni o decine di giorni, con significativa variabilità in funzione delle code di ingresso o uscita;
 - ii. per Solana (SOL), tipicamente efficaci nell'epoca successiva a quella in corso.
- e. Nei limiti consentiti dalle disponibilità di liquidità e dalle esigenze operative di CheckSig, il Cliente può richiedere l'unstaking istantaneo attraverso l'apposita funzione disponibile in Area Privata, quale opzione a pagamento. Il relativo corrispettivo è indicato nell'Informativa Corrispettivi e reso disponibile in Area Privata prima della conferma dell'operazione.

2. Custodia a Garanzia (escrow)

- a. La Custodia a Garanzia costituisce una specializzazione del Servizio di Custodia ed è prestata sulla base dei Termini di Servizio e della presente Informativa. Il servizio non è configurato come servizio autonomo disciplinato da un contratto base distinto e alternativo rispetto alla contrattualistica standard di CheckSig.
- b. Nell'ambito di operazioni di garanzia tra Clienti, CheckSig può offrire un servizio di custodia e amministrazione delle Cripto-attività vincolate in garanzia, nel rispetto dei Termini di Servizio, della presente Informativa e delle istruzioni contrattualmente applicabili alla singola operazione.
- c. Per ciascuna operazione di escrow, ai Termini di Servizio standard si affianca un contratto integrativo relativo alla specifica operazione. Tale contratto non costituisce un modello standard predisposto unilateralmente da CheckSig, ma un accordo negoziato di volta in volta tra le parti dell'operazione sottostante; CheckSig vi aderisce esclusivamente per quanto attiene al proprio ruolo di Escrow Holder.
- d. CheckSig richiede che il contratto integrativo preveda espressamente che l'Escrow Account resti regolato dai Termini di Servizio di CheckSig e che le relative previsioni abbiano funzione integrativa e prevalgano, ove difforni, limitatamente agli aspetti specifici della singola operazione.
- e. Salvo quanto diversamente previsto dal contratto integrativo applicabile, le Cripto-attività oggetto di Custodia a Garanzia restano di proprietà del Cliente titolare dell'account sul quale esse sono detenute e continuano a essere soggette ai presidi di segregazione patrimoniale, evidenza contabile distinta, identificazione, riconciliazione e tutela previsti per il Servizio di Custodia.
- f. Le modalità operative della Custodia a Garanzia possono prevedere, in funzione della struttura dell'operazione, l'utilizzo di wallet e procedure

dedicate ovvero specifiche segregazioni logiche, contabili e autorizzative all'interno dell'infrastruttura di custodia della Società. Le Cripto-attività vincolate sono in ogni caso assoggettate a presidi idonei a impedirne trasferimenti, prelievi o altre operazioni non coerenti con il vincolo di garanzia e con le istruzioni pattuite tra le parti.

- g. Il contratto integrativo può disciplinare, a titolo esemplificativo, l'individuazione di un Escrow Account dedicato, i criteri di valorizzazione delle attività, le soglie di collateralizzazione, di garanzia o di liquidazione, le margin call, i limiti alle operazioni dispositive, i casi di liquidazione automatica, la destinazione dei proventi, le modalità di rendicontazione e la cessazione del vincolo o del servizio di escrow holder. Tali profili restano disciplinati, nel loro dettaglio, dal contratto integrativo relativo alla singola operazione.
- h. CheckSig interviene esclusivamente quale Escrow Holder, nell'ambito del servizio di custodia e amministrazione di cripto-attività, e la relativa attività è limitata alla custodia e alla gestione tecnica delle Cripto-attività vincolate in garanzia, nonché all'esecuzione delle istruzioni e dei meccanismi operativi contrattualmente previsti.
- i. CheckSig non svolge attività di promozione, intermediazione, consulenza o offerta del finanziamento, né assume responsabilità in ordine alla concessione del prestito, alla valutazione del merito creditizio delle parti o all'adempimento delle obbligazioni reciproche da esse assunte nell'ambito del rapporto sottostante.

5 Modello di custodia

- 1. Il modello di custodia adottato da CheckSig si basa su un'architettura multilivello progettata per offrire elevati standard di sicurezza, segregazione, controllabilità e continuità operativa.
- 2. I wallet di Custodia di CheckSig comprendono:
 - a. deposit wallet, utilizzati per la ricezione e il transito iniziale delle Cripto-attività depositate dai Clienti;
 - b. frozen wallet, destinati alla conservazione a massima sicurezza delle Cripto-attività della clientela;
 - c. cold wallet, utilizzati per il transito controllato delle Cripto-attività in uscita dai frozen wallet;
 - d. protocol staking wallet, dedicati alle Cripto-attività vincolate in staking;
 - e. liquidity wallet, utilizzati per esigenze operative temporanee connesse ai Servizi di Trading.
- 3. CheckSig può inoltre detenere Cripto-attività presso conti aperti presso altri prestatori di servizi per le Cripto-attività autorizzati, esclusivamente nella misura necessaria all'erogazione dei Servizi di scambio ed esecuzione ordini, nel rispetto di criteri di selezione, presidi di segregazione, controlli di rischio e accordi operativi coerenti con la normativa applicabile e i Termini di Servizio.

4. I frozen wallet, i cold wallet e i protocol staking wallet sono gestiti tramite dispositivi di sicurezza hardware (HSM) e non sono direttamente accessibili tramite Internet.

5. Modello omnibus

- a. Il modello di custodia adottato da CheckSig è basato, in via ordinaria, su un modello di tipo omnibus.
- b. In tale modello, le Cripto-attività della clientela possono essere detenute in wallet condivisi o aggregati gestiti dalla Società, mentre la titolarità delle singole posizioni dei Clienti è rappresentata e ricostruita mediante evidenze contabili interne dedicate.
- c. Il Cliente prende atto che, nel modello omnibus:
 - i. non è normalmente previsto un wallet on-chain individuale separato per ciascun Cliente;
 - ii. la separazione delle posizioni della clientela è assicurata principalmente a livello giuridico, contabile, organizzativo e procedurale;
 - iii. la riconduzione delle disponibilità a ciascun Cliente avviene mediante il sistema interno di registrazione, contabilità e riconciliazione adottato da CheckSig.
- d. Il modello omnibus è adottato al fine di coniugare sicurezza, efficienza operativa, tempestività di esecuzione e continuità del servizio, fermo restando l'obbligo di CheckSig di mantenere in ogni momento evidenze idonee a identificare e ricostruire la posizione individuale di ciascun Cliente.
- e. In relazione ai Servizi di Trading, il modello omnibus può altresì agevolare la disponibilità operativa delle Cripto-attività e il netting dell'operatività complessiva della clientela, nei limiti e secondo le modalità descritte nella documentazione contrattuale e informativa.

6. Rischi specifici del modello omnibus

- a. Il modello omnibus comporta alcuni rischi specifici ulteriori rispetto ai rischi generali connessi alla detenzione e custodia di Cripto-attività.
- b. In particolare, il Cliente prende atto che il modello omnibus può comportare:
 - i. rischio di commistione operativa delle disponibilità detenute on-chain; fusione delle risorse crittografiche
 - ii. rischio di errata attribuzione o contabilizzazione delle posizioni individuali della clientela nei sistemi informativi interni; rischio di errori nella gestione dei saldi individuali
 - iii. rischio di maggiore esposizione a errori operativi centralizzati nella gestione dei saldi individuali o delle movimentazioni.
- c. Tali rischi sono mitigati da presidi contrattuali, contabili, organizzativi e tecnologici, tra cui:
 - i. il registro interno delle posizioni associato univocamente a ciascun Cliente;
 - ii. le riconciliazioni almeno giornaliere tra saldi contabili e disponibilità aggregate;

- iii. la segregazione dei ruoli e dei poteri autorizzativi;
 - iv. struttura multi-wallet al fine di bilanciare requisiti di sicurezza, liquidità operativa e tempestività di esecuzione;
 - v. procedure di autorizzazione multilivello;
 - vi. le procedure di continuità operativa, disaster recovery e restituzione;
 - vii. la rendicontazione periodica individuale e la tracciabilità delle movimentazioni.
- d. I predetti rischi non eliminano la proprietà del Cliente sulle Cripto-attività detenute in Custodia né i diritti di quest'ultimo alla restituzione, fermo restando quanto previsto dalla normativa applicabile, dai Termini di Servizio e dalle altre Informative in materia di limiti operativi, controlli di compliance, eventi tecnici, Caso Fortuito e Forza Maggiore.

6 Identificazione delle Cripto-attività e dei mezzi di accesso

1. CheckSig adotta sistemi e procedure idonei a garantire che le Cripto-attività e i mezzi di accesso alle stesse detenuti per conto della clientela siano identificati come riferibili alla custodia per conto Clienti.
2. L'identificazione avviene, a seconda dei casi, mediante:
 - a. associazione delle posizioni ai Clienti nel registro interno delle posizioni;
 - b. tracciatura delle movimentazioni e degli eventi rilevanti;
 - c. identificazione dei wallet di custodia e delle relative finalità operative;
 - d. identificazione dei mezzi di accesso crittografici, delle componenti MPC, dei dispositivi hardware di sicurezza e delle autorizzazioni come riferibili alla custodia per conto Clienti;
 - e. presidi organizzativi che distinguono le disponibilità della clientela da quelle della Società e, ove applicabile, da quelle detenute presso fornitori o CASP terzi per esigenze operative.
3. Tali sistemi sono funzionali anche alla restituzione delle Cripto-attività, alle verifiche interne, alle attività di audit e ai controlli delle Autorità competenti.

7 Esercizio dei diritti connessi alle Cripto-attività

1. CheckSig adotta sistemi e procedure che consentono ai Clienti di esercitare i diritti connessi alle Cripto-attività detenute in Custodia nei limiti della fattibilità tecnica, della conformità normativa, della sicurezza operativa e di quanto previsto dai Termini di Servizio.
2. In particolare:
 - a. il Cliente può impartire istruzioni operative tramite i canali previsti dalla documentazione contrattuale, inclusa l'Area Privata;
 - b. il Cliente riceve comunicazioni e rendicontazioni relative alla propria posizione e alle operazioni effettuate;
 - c. in presenza di eventi che richiedano una scelta, risposta o decisione del Cliente, CheckSig può mettere a disposizione informative, avvertenze o

richieste di istruzioni nei limiti in cui l'evento sia supportato e gestibile dalla Società.

3. Resta fermo che, in relazione a eventi sulla tecnologia sottostante quali fork, airdrop, split, merge, migrazioni o aggiornamenti di protocollo, il supporto di CheckSig può essere limitato o escluso nei casi previsti dai Termini di Servizio e dalla normativa applicabile, anche per ragioni di sicurezza, complessità tecnica, sostenibilità normativa o indisponibilità di fornitori o terze parti.

8 Politiche di movimentazione e restituzione

4. Le Cripto-attività possono essere movimentate esclusivamente nel rispetto di procedure di autorizzazione predefinite e dei controlli di rischio e compliance applicabili.
5. I depositi sono trasferiti dai *deposit wallet* ai *frozen wallet* solo dopo il completamento dei controlli di conformità.
6. I prelievi richiedono autorizzazioni multiple, incluso un quorum di agenti terzi per ridurre il rischio di operazioni fraudolente, e possono essere soggetti a controlli ulteriori in funzione dell'importo, del profilo di rischio, della novità e dell'indirizzo di destinazione, della normativa AML/CFT, delle sanzioni e delle policy interne.
7. CheckSig si impegna a restituire le Cripto-attività della stessa specie e quantità su richiesta del Cliente o alla cessazione del Contratto, nei limiti e secondo quanto previsto dai Termini di Servizio e dalla normativa applicabile.
8. In caso di cessazione del Contratto, CheckSig esegue il trasferimento delle Cripto-attività entro il Tempo tecnico di disponibilità delle Cripto-attività (fino a 10 giorni lavorativi; in condizioni operative ordinarie la disponibilità è usualmente immediata — cfr. art. 2.22 dei Termini di Servizio).
9. La restituzione può avvenire mediante trasferimento verso indirizzi esterni comunicati dal Cliente, da lui controllati direttamente o a lui intestati presso intermediari, nel rispetto delle verifiche di sicurezza e compliance previste.
10. Non sono consentiti depositi, prelievi o trasferimenti di Electronic Money Token, secondo quanto previsto dai Termini di Servizio e dalle Informative applicabili.

9 Attestazione pubblica delle riserve

1. Con frequenza almeno mensile, CheckSig pubblica una Proof-of-Reserves, intesa come attestazione pubblica verso l'esterno finalizzata a consentire verifiche indipendenti sulla disponibilità delle Cripto-attività detenute in custodia.
2. La Proof-of-Reserves si basa su evidenze verificabili pubblicamente, quali informazioni e transazioni tracciabili sulle blockchain di riferimento e documentazione resa disponibile da CheckSig.
3. L'attestazione consente di verificare la riconducibilità degli indirizzi e dei saldi delle Cripto-attività agli ambienti di custodia di CheckSig e supporta le attività di controllo e riconciliazione.

4. La Proof-of-Reserves attesta elementi di disponibilità e controllabilità delle Cripto-attività in custodia, ma non costituisce attestazione individuale della posizione del singolo Cliente.
5. La Proof-of-Reserves non rappresenta un bilancio, né una verifica delle passività o degli impegni di CheckSig verso i Clienti. Pertanto, non costituisce una certificazione contabile né una garanzia di solvibilità, ma uno strumento di trasparenza verificabile.

10 Gestione degli incidenti informatici

1. CheckSig adotta un sistema strutturato di gestione degli incidenti informatici e operativi rilevanti, basato su:
 - a. tempestiva identificazione e classificazione degli eventi;
 - b. attivazione di procedure di contenimento e mitigazione;
 - c. tracciamento e registrazione in apposito registro interno;
 - d. analisi delle cause e definizione di misure correttive e preventive;
 - e. comunicazione agli utenti interessati, ove possibile entro termini coerenti con quanto previsto dai Termini di Servizio;
 - f. comunicazione alle autorità competenti, ove richiesto dalla normativa applicabile.
2. In caso di incidente che possa incidere sulla disponibilità, integrità o sicurezza delle Cripto-attività detenute in custodia, CheckSig attiva procedure di emergenza volte alla protezione dei fondi e alla continuità operativa e, ove applicabile, alla restituzione o movimentazione controllata delle disponibilità.

11 Rischi tecnologici, operativi e di mercato delle Cripto-attività

1. La Custodia e l'amministrazione di Cripto-attività comportano rischi tecnologici, operativi e di mercato intrinseci alla natura delle Cripto-attività e delle tecnologie a registro distribuito (DLT), che non dipendono dalla prestazione del servizio di custodia in quanto tale.
2. In particolare, restano integralmente applicabili e richiamati i rischi descritti nei Termini di Servizio e nelle altre Informative applicabili, inclusi, a titolo esemplificativo e non esaustivo:
 - a. volatilità dei prezzi delle Cripto-attività, che possono determinare variazioni anche significative e improvvise del loro valore economico;
 - b. malfunzionamenti, congestioni o vulnerabilità delle reti blockchain e dei protocollo DLT;
 - c. irreversibilità delle transazioni, per cui operazioni confermate sul registro distribuito non possono essere annullate o modificate;
 - d. fork, aggiornamenti di protocollo o modifiche delle regole di consenso, che possono incidere sul funzionamento della rete, sulla disponibilità delle Cripto-attività o sulle tempistiche operative;
 - e. rischi di controparte, custodia presso terzi e dipendenza da fornitori o CASP;

- f. rischi di interruzione, rallentamento o indisponibilità temporanea delle reti, indipendenti dalla volontà o dal controllo di CheckSig.
3. Tali rischi non sono eliminabili né mitigabili integralmente da CheckSig e non costituiscono di per sé inadempimento del servizio di custodia, fermo restando quanto previsto in materia di responsabilità nei casi di perdita imputabile al servizio prestato, ai sensi dei Termini di Servizio e della normativa applicabile.

12 Responsabilità

1. CheckSig è responsabile, nei limiti e secondo quanto previsto dalla normativa applicabile, inclusi gli articoli 75 e 82 MiCAR, per la perdita di Cripto-attività o dei mezzi di accesso ad esse associati detenuti in Custodia, qualora tale perdita sia imputabile a violazioni o carenze del servizio di custodia. In tali casi, CheckSig provvede, ove possibile, alla restituzione di Cripto-attività della stessa specie e quantità o del relativo controvalore, secondo quanto previsto dalla normativa applicabile.
2. Resta fermo che non sussiste responsabilità qualora la perdita sia dovuta a evento esterno non imputabile a CheckSig, a Caso Fortuito, Forza Maggiore o a condotte, errori od omissioni del Cliente, nei limiti consentiti dalla normativa applicabile.
3. Le coperture assicurative sono strutturate in modo da proteggere la Società e, indirettamente, i Clienti rispetto a specifici rischi operativi, inclusi, a titolo esemplificativo, eventi di natura informatica, frodi interne o esterne, errori operativi e altri eventi che possano determinare perdite patrimoniali connesse al servizio di custodia, nei limiti, alle condizioni e secondo i massimali previsti dalle relative polizze.
4. Le eventuali coperture assicurative costituiscono uno strumento di mitigazione del rischio e non limitano i diritti inderogabili del Cliente previsti dalla normativa applicabile.
5. Le informazioni aggiornate in merito alle coperture assicurative in essere, inclusi l'identità dell'assicuratore e i principali massimali, sono rese disponibili nella sezione dedicata del Sito.

-
- **Nome documento:** informativa-custodia
 - **Stato:** Approvato
 - **Organo approvante:** Consiglio di amministrazione
 - **Data di approvazione:** 2026-06-26

Storico delle versioni

Versione	Changelog
2.4.1	• Rimossa dal punto 2.3.d la frase "salvo consenso espresso del Cliente o quanto specificamente previsto dalla normativa applicabile e dalla documentazione contrattuale".

	• Adeguato il riferimento alla definizione aggiornata di “Tempo tecnico di disponibilità delle Cripto-attività”
2.4.0	• Rafforzamento della descrizione dei presidi organizzativi, contabili e tecnologici, incluse riconciliazioni giornaliere, tracciabilità delle movimentazioni e possibile detenzione operativa presso CASP terzi • Ampliamento e sistematizzazione della disciplina della custodia a garanzia (escrow) e dello staking protocolare • Introduzione di sezioni dedicate a identificazione delle cripto-attività e dei mezzi di accesso, esercizio dei diritti connessi alle cripto-attività, politiche di movimentazione e restituzione • Chiarimenti su rischi di controparte, continuità operativa e regime di responsabilità ai sensi della normativa applicabile
2.3.0	• Esplicitazione del modello omnibus e descrizione dei relativi rischi • Revisione generale del wording relativo alla restituzione, riconciliazione, identificazione dei mezzi di accesso e custodia a garanzia
2.2.0	1) Introdotti chiarimenti negli artt. 2 e 3 per esplicitare presidi ed evidenze operative relativi a: (i) esercizio dei diritti connessi alle cripto-attività detenute, (ii) restituzione delle cripto-attività al Cliente, (iii) identificazione delle cripto-attività e dei mezzi di accesso detenuti per conto della clientela. 2) Aggiornamenti di coordinamento redazionale per coerenza del pacchetto informativo.
2.1.0	Revisione del pacchetto contrattuale per maggiore coerenza tra i diversi documenti