

Polizza di Assicurazione per la protezione dei dati biometrici

Impresa di Assicurazione: UNIQA VERSICHERUNG AG impresa in regime di libera prestazione di servizi

Ed. Marzo 2024

Prodotto: "Wallife Biometrics ID Smart"

Sommar

NORME COMUNI A TUTTE LE GARANZIE	6
1. OGGETTO DELL'ASSICURAZIONE	6
2. RISCHI ESCLUSI.....	6
3. DICHIARAZIONI RELATIVE ALLE CIRCOSTANZE INFLUENTI SULLA VALUTAZIONE DEL RISCHIO.....	7
3.1. DIMINUZIONE E AGGRAVAMENTO DEL RISCHIO	7
3.2. MODIFICHE DELL'ASSICURAZIONE	7
3.3. ALTRI CONTRATTI ASSICURATIVI	7
4. FORMA DELLE COMUNICAZIONI	7
5. TITOLARITÀ DEI DIRITTI NASCENTI DALLA POLIZZA	7
6. TERMINE DI PRESCRIZIONE	7
7. CLAUSOLA DI INOPERATIVITÀ DELLA COPERTURA PER SANZIONI INTERNAZIONALI.....	7
8. LEGGE APPLICABILE E FORO COMPETENTE	7
9. CALCOLO DEL PREMIO	8
9.1. ONERI FISCALI.....	8
9.2. PAGAMENTO DEL PREMIO.....	8
10. DURATA DELLA POLIZZA	8
10.1. EFFICACIA ED EFFETTO DELLA COPERTURA	8
11. DIRITTO DI RECESSO	8
12. RISOLUZIONE DEL CONTRATTO	8
SEZIONE PERDITE PECUNIARIE	9
13. PROTEZIONE IDENTITÀ DIGITALE	9
14. RISCHI ESCLUSI.....	9
15. FRANCHIGIE, MASSIMALE E LIMITI DI INDENNIZZO/RIMBORSO.....	10
15.1. RIEPILOGO DI FRANCHIGIE E LIMITI DI INDENNIZZO/RIMBORSO.....	10
16. EFFICACIA / VALIDITÀ TERRITORIALE DELL'ASSICURAZIONE.....	10
17. CHE COSA FARE IN CASO DI SINISTRO?	10
17.1. OBBLIGHI DELL'ASSICURATO – AVVISO DI SINISTRO - SERVIZIO DI CONTACT CENTER	11
17.2. PAGAMENTO DELL'INDENNIZZO PER LE GARANZIE PRESTATE NELLA SEZIONE PERDITE PECUNIARIE CHE PREVEDANO IL RIMBORSO ALL'ASSICURATO.....	12
17.3. INOSSERVANZA DEGLI OBBLIGHI RELATIVI AI SINISTRI	12
17.4. ESAGERAZIONE DOLOSA DEL DANNO	12
17.5. VALUTA DEI PAGAMENTI.....	12
ALLEGATO 1	13

GLOSSARIO

Ai seguenti termini la Società ed il Contraente attribuiscono convenzionalmente questi significati:

Anno assicurativo: periodo di tempo pari a 365 giorni, o a 366 giorni in caso di anno bisestile, che decorre dalla data di stipula della polizza.

APP o Wallife APP o applicazione mobile: Applicazione mobile che consente di mitigare il rischio di sottrazione fraudolenta delle credenziali di accesso allo smartphone. L'applicazione consente anche la gestione digitale del contratto.

Apparato Digitale "Home": Apparecchi di rete fissa quali ad esempio computer, desktop, stampanti (sia wifi che usb), fax, scanner e multifunzione (cioè apparati che abbiano funzione di stampa, scansione e fax), webcam, router e chiavette, smart tv, decoder, consolle da gaming, dispositivi di smarthome, di uso privato e di proprietà dell'assicurato.

Tale elenco è soggetto ad aggiornamenti/implementazioni legati ad eventuali sviluppi tecnologici che portino alla commercializzazione di nuovi dispositivi elettronici.

Apparato Digitale "Mobile": Apparecchi mobili quali ad esempio computer portatili (notebook, laptop), tablet, phablet, smartphone, smartwatch; di uso privato e di proprietà dell'assicurato.

Tale elenco è soggetto ad aggiornamenti/implementazioni legati ad eventuali sviluppi tecnologici che portino alla commercializzazione di nuovi dispositivi elettronici.

Apparato Digitale connesso: Apparato digitale "Home" o "Mobile" collegato ad una rete internet.

Assicurato: soggetto il cui interesse è protetto dall'assicurazione.

Assistenza Digitale: Attività che ha come scopo il ripristino, causa malfunzionamento, dell'operatività di un Apparato Digitale o software, incluso il supporto all'installazione e/o la loro (ri)configurazione. Tale operazione può avvenire tramite l'Assistenza in remoto o per mezzo di Assistenza tecnica a domicilio.

Assistenza in remoto: Tipo di Assistenza Digitale che viene fornita telefonicamente, (con o senza il supporto di software dedicati come cobrowsing o videobrowsing), via chat oppure tramite mail. Si specifica che per garantire un intervento da remoto con buona qualità audio/video sarà necessaria una connessione almeno 2 mbps download, 0,80 mbps upload.

Autenticazione a più fattori: L'utilizzo di due o più dei seguenti fattori per verificare l'identità di un utente: fattore di conoscenza, "qualcosa che un individuo conosce"; fattore di possesso, "qualcosa che un individuo possiede"; fattore biometrico, "qualcosa che un individuo è o è in grado di fare".

Cobrowsing: Software di assistenza tecnica evoluto che permette all'operatore di prendere possesso dell'apparato del cliente (ad esempio Pc) ed operare direttamente sullo stesso al fine di configurarlo o cambiarne le impostazioni.

Commercio elettronico (e-commerce): l'insieme delle transazioni per la commercializzazione di beni e servizi tra venditore (offerta) e consumatore (domanda), realizzate tramite Internet.

Compagnia di Assicurazione o Compagnia: UNIQA VERSICHERUNG AG - Sede Legale AUSTRASSE 46 - 9460 VADUZ LIECHTENSTEIN. Iscritta nel registro delle imprese e delle società del LIECHTENSTEIN con il numero FL-0001.522.928-1. Società sottoposta alla vigilanza dell'Autorità del Liechtenstein preposta alla regolamentazione dei servizi finanziari e abilitata all'esercizio dell'attività Assicurativa in Italia in libera prestazione di servizi. Iscritta il 2.11.2009, al nr. II.00846, all'appendice dell'albo Imprese Assicuratrici (Elenco II) dell'IVASS, limitatamente ai rischi perdite pecuniarie e tutela legale;

Compagnia di Assicurazione assistenza o Compagnia di assistenza: Inter Partner Assistance S.A. – Rappresentanza Generale per l'Italia - Gruppo AXA Partners – Via Carlo Pesenti 121 – 00156 Roma - Iscritta in Italia all'albo imprese IVASS n. I.00014 - Registro delle Imprese di Roma RM Numero REA 792129 - Part. I.V.A. 04673941003 - Cod. Fisc. 03420940151

Conto: conto corrente bancario, un libretto di risparmio (o altra forma di deposito di risparmio), un conto di deposito di mercato monetario, un deposito rimborsabile a vista (deposito a risparmio libero) [o a scadenza/con preavviso], la posizione individuale della previdenza complementare, di cui sia titolare un Assicurato e che sia gestito direttamente o indirettamente da un'Istituzione Finanziaria, costituito al fine di essere utilizzato per scopi personali, familiari o generalmente attinenti la vita privata.

Controparte: la parte avversaria in una controversia.

Contraente: soggetto che stipula la polizza assicurativa.

Danno accidentale: Il danno esteriormente constatabile, direttamente provocato da cause esterne, quali cadute o altri urti o rotture accidentali, che pregiudichi il funzionamento dell'Apparecchio garantito.

Danno di natura contrattuale: danno conseguente all' inadempimento di una obbligazione assunta da chi ha stipulato un contratto.

Danno extracontrattuale: danno a cose o a persona subito in occasione di un fatto illecito commesso da un soggetto terzo.

Danni materiali: la distruzione, il danneggiamento, il pregiudizio al funzionamento, la perdita di valore o la perdita di beni mobili o immobili, come pure i danni patrimoniali che ne derivano per il danneggiato. Sono considerati Danni Materiali anche la morte, il ferimento o altri danni salute, nonché la perdita di animali.

Danno da Sottrazione di Fondi: la Perdita sofferta dall'Assicurato e causata da un Trasferimento elettronico non autorizzato di fondi, equivalente all'ammontare dei fondi ovvero dei soldi, esclusi interessi e commissioni, oggetto di tale trasferimento.

Delitto colposo: atto illecito di rilevanza penale commesso per negligenza, imperizia, imprudenza o inosservanza di leggi, ma senza volontà né intenzione di causare l'evento lesivo.

Delitto doloso: atto illecito di rilevanza penale commesso con volontà e intenzione di causare l'evento lesivo, diversamente dal delitto colposo.

Derubricazione del reato: qualificazione giuridica del reato diversa da quella inizialmente enunciata nell'imputazione (per esempio da doloso a colposo).

Distributore: il soggetto che, dietro accordo con l'intermediario, si occupa del collocamento del prodotto

Diritti reali: diritti che rappresentano in un soggetto la titolarità del rapporto giuridico esclusivo su un bene di rilevanza giuridica ed economica (es. proprietà, usufrutto).

Disdetta: atto con il quale viene comunicata l'intenzione di non rinnovare, alla scadenza, la polizza assicurativa.

Dispositivi di smarthome: IPcam, sensori apertura/chiusura porte, smart switch, sensori di fumo, sensori di allagamento, termostato, valvole termostatiche, sensori di temperatura, sensori di movimento, lampadine intelligenti, serratura elettronica.

Fase giudiziale: fase nella quale ci si rivolge all'Autorità giudiziaria per definire una controversia.

Fase stragiudiziale: fase della controversia nella quale non ci si è ancora rivolti all'Autorità giudiziaria, perché si sta tentando una possibile definizione bonaria della vertenza.

Fatto illecito: l'azione o l'omissione contraria all'ordinamento giuridico in quanto violazione di un dovere o di un obbligo imposti da una norma di legge

Fibra: Servizio telefonico-internet che si avvale dell'utilizzo della fibra ottica. Porta a casa dell'utente un servizio dati e quindi necessita di un router capace di utilizzare questo tipo di segnale, tipicamente un apparato voip fornito dal gestore

Franchigia: importo fisso che rimane a carico dell'Assicurato. Se non è indicato in modo diverso, si applica per Evento.

Esempio di applicazione della franchigia:

Franchigia = €100,00;

Spese sostenute dall'Assicurato = € 500,00;

Spese rimborsate all'Assicurato = € 400,00.

Furto di identità digitale: furto di elementi identificativi dell'Assicurato verificatosi o derivante dall'utilizzo dello smartphone da parte di quest'ultimo. Per elementi identificativi si intende, a titolo esemplificativo, il nominativo dell'Assicurato, il Codice fiscale (o altro numero identificativo equivalente di assistenza sociale, emesso da un governo), o di qualsivoglia altro metodo o elemento di identificazione dell'Assicurato, che ha o potrebbe ragionevolmente comportare l'uso illecito di tali informazioni. Un Furto di Identità non include il furto o l'uso non autorizzato o illegale della ragione sociale e / o qualsiasi altro segno distintivo o metodo di identificazione della propria attività commerciale.

Impianto domestico: In ambito digitale l'insieme di cavi e prese telefoniche nell'abitazione che ricevono il servizio dsl o fibra dall'esterno e lo trasmettono all'interno dell'abitazione. Tale servizio è generalmente garantito dal gestore del servizio telefonico solo fino alla prima presa (la più vicina rispetto all'ingresso dell'abitazione), il resto dell'impianto è responsabilità del cliente. Alcune volte l'impianto riceve invece il segnale da una sim dati. In ambito di assistenza digitale può essere necessario mandare un tecnico a riparare, modificare o potenziare l'impianto domestico al fine di estendere il servizio ad alcuni ambienti della casa, o migliorarne la fruibilità.

Intermediario emittente: Wallife Insurance S.r.l. – RUI A000710058 sede legale Via Vittorio Veneto 116, 00187 – Roma – Italia, Codice Fiscale 16592051003

Istituzione Finanziaria: istituto di credito, una banca, una banca di credito cooperativo, fondo pensione integrativo o qualsiasi altra entità che direttamente o indirettamente detiene un Conto appartenente all'Assicurato, o che emette un Dispositivo di Accesso e concorda con l'Assicurato di prestare un servizio di Trasferimento di fondi, che sia in entrambi i casi autorizzata ad operare in Italia.

IVASS (precedentemente denominato ISVAP): Istituto per la Vigilanza sulle assicurazioni, autorità pubblica indipendente che svolge la funzione di vigilanza sul rispetto delle norme che regolano l'attività assicurativa e di intermediazione assicurativa.

Malfunzionamento: il mancato funzionamento oppure il funzionamento difettoso o inadeguato di un Apparato Digitale "Home" e "Mobile" o della Rete Domestica, che non ne permetta le prestazioni abituali e conformi all'uso previsto dal venditore ma che non sia legato ad un danno accidentale.

Manutenzione: l'insieme delle operazioni che vanno effettuate per tenere sempre in buono stato e nella dovuta efficienza funzionale i beni oggetto di manutenzione, in rispondenza agli scopi per cui sono stati costruiti.

Massimale: La somma massima liquidabile da UNIQA AG.

Esempio di applicazione del massimale e dello scoperto:

Massimale = € 5.000 insieme a scoperto = 25%;

• spese sostenute dall'Assicurato = € 4.000; spese rimborsate all'Assicurato = € 3.000 (4.000 - 1.000), poiché rimane a carico dell'Assicurato lo scoperto del 25% di € 4.000; non opera il massimale;

• spese sostenute dall'Assicurato = € 8.000; spese rimborsate all'Assicurato = € 5.000 poiché opera dapprima lo scoperto (8.000 - 25% = € 6.000) e successivamente il massimale (€ 5.000).

Massimale per anno assicurativo: somma massima liquidabile dalla Società per i danni conseguenti a sinistri insorti nello stesso anno assicurativo, anche se denunciati in momenti diversi, limitatamente agli oneri previsti dalla polizza assicurativa.

Massimale per caso assicurativo: somma massima liquidabile dalla Società per ogni caso assicurativo denunciato limitatamente agli oneri previsti dalla polizza assicurativa.

Media network: tecnologie e pratiche online utilizzate per condividere contenuti testuali, notizie, informazioni, immagini, video e audio

Mediazione: istituto giuridico introdotto con il Decreto Legislativo n. 28 del 4 marzo 2010, per la composizione di determinate tipologie di controversie tra le parti.

Negoziante assistita: accordo disciplinato dal Decreto-legge n. 132 del 12 settembre 2014, mediante il quale le parti convengono di cooperare in buona fede e con lealtà per risolvere in via amichevole la controversia tramite l'assistenza professionale di avvocati.

Organismo di mediazione: Organismo creato da soggetti pubblici e privati cui la legge affida la gestione del procedimento di mediazione. Gli Organismi di mediazione sono iscritti in un apposito Registro presso il Ministero della giustizia, consultabile nel sito del medesimo Ministero.

Periodo di tolleranza: il numero di giorni, indicato sulla scheda di polizza, durante i quali la copertura assicurativa continua ad operare anche se il contraente non ha pagato alla scadenza convenuta la rata di premio successiva alla prima o il premio di rinnovo di una polizza con tacito rinnovo

Perito: Libero professionista incaricato dall'impresa di assicurazione di stimare l'entità del danno provocato dal sinistro.

Phishing: metodo ingannevole che spinge gli utenti a rivelare password, numeri di carte di credito e altre informazioni sensibili utilizzato

da criminali che si spacciano per una istituzione legittima via e-mail, SMS o chiamate vocali. A titolo esemplificativo ma non esaustivo sono considerati tentativi di phishing le seguenti modalità di truffa: SMISHING, VISHING, WHALING

Polizza: il documento contrattuale che disciplina i rapporti tra Società, Contraente e Assicurato, che riporta del Condizioni di Assicurazione.

Premio: somma dovuta alla Società dal Contraente a corrispettivo della garanzia assicurativa.

Provider: il fornitore che provvede alle operazioni di cancellazione e rimozione dei contenuti digitali lesivi della reputazione dai social e dalla rete internet

Rete domestica; Insieme delle connessioni wifi generate dagli apparati dell'utente nell'ambiente domestico, e dell'impianto domestico stesso.

Rete Wifi: Modalità di collegamento ad internet senza cavi o fili di apparati. Tipicamente un apparato (router) si collega ad internet tramite rete fissa (DSL o fibra) o sim dati e genera un campo wifi a cui altri apparati si agganciano per condividere il collegamento (o connessione) ad internet del primo. Tale rete può essere protetta (gli apparati per collegarsi devono utilizzare una password) o libera. Le dimensioni e la potenza di una rete wifi variano, sono influenzati tra l'altro dallo spessore delle mura o da interferenze quali altre reti simili vicine.

Scoperto: percentuale del danno che resta a carico dell'Assicurato. Si applica per ogni sinistro, se non è convenuto diversamente.

Esempio:
Scoperto = 25%;
Danno subito dall'Assicurato = € 4000; Spese rimborsate all'Assicurato = € 3000 poiché rimane a carico dell'Assicurato il 25% del danno (€ 1000).

Sinistro: l'evento da cui consegue il danno economicamente apprezzabile, per il quale è prestata l'assicurazione.

Sistema di sicurezza: software o hardware che fornisca almeno una protezione preventiva contro: virus e malware, phishing e smishing (link e siti web dannosi), connessioni non sicure quando si accede a siti web di operazioni bancarie e di pagamento.

L'assicurato ha il diritto di utilizzare un sistema di sicurezza di sua scelta, purché fornisca il livello minimo di protezione sopra descritto. A titolo di esempio, può sceglierne uno tra quelli distribuiti da: AVG, Bitdefender, Kaspersky, McAfee, Norton, Panda.

Smishing: Lo smishing è un attacco che, per la sua esecuzione, utilizza i messaggi di testo o SMS. Una tecnica comune di smishing consiste nell'inviare ad un telefono cellulare tramite SMS un messaggio che contiene un collegamento cliccabile o un numero di telefono da richiamare.

Un esempio comune di attacco di smishing è un messaggio SMS che sembra provenire dal proprio istituto bancario. Il contenuto afferma che il conto è stato compromesso e che è necessario rispondere immediatamente. L'attaccante chiede di verificare numero di conto corrente bancario, codice fiscale, ecc. Una volta che l'aggressore riceve le informazioni, acquisisce il controllo del conto bancario.

Spettrometro: Software di assistenza che permette, tramite lo smartphone del cliente, di analizzare i canali wi-fi presso il domicilio del cliente al fine di eliminare problemi dovuti a più wifi attivi sullo stesso canale, ed ottimizzare l'utilizzo degli apparati.

Strong Customer Authentication (SCA): sistema di autenticazione dell'utente attraverso l'utilizzo di almeno due dei seguenti elementi:

- a) identificazione con una password o con un PIN;
- b) identificazione attraverso un device come lo smartphone o un device portatile o ancora un token bancario;
- c) identificazione attraverso l'impronta digitale o lineamenti biometrici del viso, ovvero tratti che, in qualche modo, sono in grado di caratterizzare il cliente identificandolo nella sua persona in modo univoco.

Tokenizzazione della carta di credito: sistema utilizzato per proteggere le carte di credito. Lo strumento di tokenizzazione è utilizzato per evitare la duplicazione dei dati di un titolare di una carta.

Transazione: accordo con il quale le parti, facendosi reciproche concessioni, pongono fine ad una lite tra di loro insorta o la prevengono

Trasferimento elettronico di fondi: il trasferimento di fondi, avviati attraverso un terminale elettronico, uno smartphone, o un computer effettuato allo scopo di ordinare, istruire o autorizzare l'Istituzione Finanziaria ad addebitare o accreditare il Conto di un Assicurato.

Il trasferimento elettronico di fondi include, a titolo esemplificativo ma non esaustivo:

- i trasferimenti effettuati tramite dispositivi EFT-POS presenti presso i punti vendita;
- i trasferimenti o prelievi effettuati tramite bancomat;
- versamenti o prelievi di fondi;
- trasferimenti disposti tramite smartphone;
- trasferimenti derivanti da transazioni effettuate per il tramite di carte di debito o di credito, effettuate tramite un terminale elettronico.

Trasferimento elettronico non autorizzato di fondi: Trasferimento di fondi effettuato elettronicamente dal Conto dell'Assicurato eseguito da una persona terza senza autorizzazione. Non costituisce Trasferimento Elettronico non autorizzato di Fondi (TEAF) quello eseguito:

- 1) da una persona a cui l'Assicurato abbia fornito il Dispositivo di Accesso al proprio Conto o le credenziali dello stesso, a meno che non si sia preventivamente notificato all'Istituto Finanziario che i trasferimenti effettuati da tale persona non siano più autorizzati e l'Istituzione Finanziaria sia in grado di individuarli;
- 2) con intento fraudolento da parte dell'Assicurato o di qualsiasi persona che agisca di concerto con lo stesso;
- 3) dall'Istituzione Finanziaria o dal suo dipendente; o
- 4) da qualsiasi conto relativo ad un'attività imprenditoriale o commerciale.

Ultimo miglio: Termine che si utilizza nelle telecomunicazioni per identificare l'ultimo parte della tratta di cavo (rame o fibra) che porta il servizio telefonico a casa del cliente. Il termine identifica la tratta che specificatamente va dall'armadio di strada alla prima presa telefonica dell'impianto domestico.

Vishing: Tipologia di attacco di phishing eseguito tramite una chiamata vocale.

Un esempio di attacco di vishing include una chiamata da parte di criminali che dichiarano di essere impiegati della vostra banca e vi comunicano un problema o un blocco sul vostro conto o sulla vostra carta. Vi chiedono di dimostrare che siete i legittimi proprietari fornendo i dati completi delle carte o del conto bancario in modo che possano controllarli nei loro database. A volte vi chiedono anche di fornire loro il codice di sicurezza che avete appena ricevuto via SMS, per verificare che il vostro telefono funzioni correttamente. O il PIN della vostra carta. Tutte queste informazioni consentono loro di effettuare acquisti online o trasferimenti fraudolenti a vostro nome.

Videobrowsing: Software di assistenza tecnica evoluto che permette all'operatore di utilizzare la videocamera o la fotocamera dello smartphone del cliente per assisterlo in caso di sinistro.

Whaling: tipo di phishing che prende di mira un CEO, un CFO o qualsiasi manager apicale di un settore o di una specifica azienda.

Un esempio di whaling include l'invio di un'e-mail che afferma che l'azienda sta per incorrere in conseguenze legali e che è necessario cliccare sul collegamento per ottenere maggiori informazioni.

Il collegamento porta quindi a una pagina che richiede di inserire tutti i dati critici dell'azienda, come codice fiscale e numeri dei conti correnti bancari.

NORME COMUNI A TUTTE LE GARANZIE

Norme valide per tutte le garanzie prestate dall'assicurazione



Che cosa è assicurato?

1. OGGETTO DELL'ASSICURAZIONE

Wallife® Biometrics ID è la polizza che protegge l'assicurato dal furto dell'identità digitale, tutela la sua reputazione online e garantisce un rimborso in caso di sottrazione illecita di denaro da conti correnti e strumenti di pagamento.

In cosa consiste il furto dell'identità digitale?

Per furto dell'identità digitale s'intende l'acquisizione e l'utilizzo illecito delle informazioni personali e riservate, mediante accesso non autorizzato, anche da remoto, ad un Apparato Digitale dell'assicurato connesso in rete (smartphone, tablet e pc).

Quali sono le informazioni personali dell'assicurato?

Per informazioni personali dell'assicurato s'intende: il suo nome, il codice fiscale (o qualunque altro numero identificativo equivalente di assistenza sociale, rilasciato da un governo), e-mail e password, credenziali di accesso a strumenti di pagamento o account social o qualsiasi elemento di identificazione personale per accedere a servizi online, che potrebbero essere utilizzate illegalmente.

Quali sono le condizioni per ottenere un rimborso?

Affinché l'assicurato ottenga il rimborso del sinistro, il furto dell'identità digitale deve essere commesso mediante accesso non autorizzato agli Apparati Digitali connessi dell'Assicurato attraverso:

- a) malware o virus;
- b) una delle seguenti tecniche di social-engineering: phishing (una e-mail o un'altra comunicazione fraudolenta inviata allo scopo di attirare una vittima), smishing (ad esempio un messaggio SMS che sembra provenire dal proprio istituto bancario, il cui contenuto afferma che il conto è stato compromesso e che è necessario rispondere immediatamente) ed e-mail spam (l'invio di messaggi di posta elettronica pubblicitari truffaldini).
- c) la compromissione dei Apparati Digitali connessi ad una rete Wi-Fi pubblica tramite lo sfruttamento di vulnerabilità degli stessi Apparati Digitali connessi;
- d) la compromissione della rete Wi-Fi utilizzate dagli Apparati digitali connessi dell'Assicurato;
- e) l'utilizzo di Backdoor;
- f) linee di trasmissione a seguito di Autenticazione avvenuta con l'utilizzo di credenziali ottenute tramite attacchi di Brute Force o per mezzo di tecniche di Keylogging.

Quali sono le condizioni affinché la copertura assicurativa sia valida?

La copertura assicurativa è valida a condizione che:

- L'Assicurato sia in grado di individuare e provare che il furto di identità digitale sia avvenuto mediante accesso non autorizzato, ad esempio allegando la mail di phishing ricevuta;
- Gli Apparati Digitali connessi siano costantemente aggiornati;
- Gli Apparati Digitali connessi utilizzati dall'utente per le attività e i pagamenti online, siano dotati di un sistema di sicurezza valido e aggiornato;
- L'Assicurato adotti, dove possibile, tecniche di autenticazione a due fattori (2FA) o, in alternativa, effettui regolarmente la modifica delle password di accesso.

La polizza offre, inoltre, la possibilità di proteggere la propria identità digitale presente anche grazie all'utilizzo dell'App Wallife, un'applicazione mobile che consente di mitigare il rischio di furto di dati e conseguenti perdite di denaro. L'App Wallife, disponibile gratuitamente su Apple AppStore e Google PlayStore, contribuisce a proteggere l'assicurato attraverso:

- Scan Wallife: rileva più di 60 minacce presenti nello smartphone, nella rete e nelle app installate.
- Anti-Phishing: verifica l'affidabilità di pagine web, link, SMS, QR code, e-mail e documenti.
- Data Breach Checker: monitora la violazione di dati personali, come e-mail e numeri di telefono.
- Moni-Thor: avvisa l'Assicurato in caso di utilizzo dello smartphone diverso dall'utente abituale.



Che cosa non è assicurato?

2. RISCHI ESCLUSI

Resta escluso dalla garanzia prestata con l'assicurazione ogni sinistro derivante direttamente od indirettamente:

- a) dal mancato aggiornamento del software presente sugli Apparati digitali dell'Assicurato, quando richiesto dal fornitore;
- b) dalla mancanza di un sistema di sicurezza valido attivo sugli Apparati digitali connessi dell'Assicurato;
- c) dall'eliminazione delle restrizioni software imposte dal produttore (c.d. jailbreak o root), ovvero dalla forzatura dell'Apparato digitale per bypassare le restrizioni imposte dal produttore al fine di modificare il software preinstallato;
- d) da colpa grave dell'assicurato, intendendosi per colpa grave la consapevole e volontaria inosservanza da parte dell'Assicurato o da chi utilizzi il prodotto assicurato dell'ordinaria diligenza richiesta;
- e) da qualsiasi atto compiuto dall'Assicurato in violazione di divieti o regolamenti governativi;
- f) da pubblicazione di contenuti su siti web in cui tali contenuti possono essere pubblicati senza registrazione delle credenziali

- d'accesso, oppure su siti web che non sono direttamente controllati dall'Assicurato;
- g) da mancata rimozione, a seguito di denuncia o richiesta da parte di terzi, di contenuto, da siti o pagine web che siano sotto il diretto controllo dell'Assicurato;
 - h) da furto, violazione o divulgazione di informazioni, documenti o dati coperti dal diritto di proprietà intellettuale;
 - i) dalla perdita o dallo smarrimento dello smartphone o dai danni materiali allo stesso che comportino perdita dei dati.



Che obblighi ho? Quali obblighi ha l'impresa

3. DICHIARAZIONI RELATIVE ALLE CIRCOSTANZE INFLUENTI SULLA VALUTAZIONE DEL RISCHIO

Il Contraente, prima della sottoscrizione della polizza, informa la Compagnia sulle condizioni del rischio da assicurare e lo aggiorna anche successivamente sulle circostanze ed i mutamenti che possono influire su dette condizioni del rischio, in modo che l'assicuratore possa prestare la garanzia assicurativa e determinarne il premio in base allo stato del rischio come rappresentato dal Contraente.

Le dichiarazioni del Contraente, pertanto, riportano alla Compagnia quanto a sua conoscenza sullo stato del rischio da assicurare, senza reticenze o inesattezze. Al riguardo si applicano gli articoli 1892 e 1893 del Codice Civile, secondo i quali le dichiarazioni che risultino inesatte e reticenti e siano state rese dal Contraente con dolo o colpa grave possono comportare la perdita totale del diritto all'indennizzo o alla prestazione; mentre invece le dichiarazioni rese od omesse senza dolo o colpa grave possono comportare la riduzione dell'indennizzo in proporzione all'eventuale maggior premio rischio dal reale stato del rischio.

3.1. DIMINUZIONE E AGGRAVAMENTO DEL RISCHIO

Il Contraente comunica alla Compagnia le variazioni che comportano una diminuzione o un aggravamento del rischio.

In seguito alla comunicazione del Contraente si applicano rispettivamente l'art. 1897 Codice civile in caso di diminuzione del rischio, e l'art. 1898 in caso di aggravamento.

3.2. MODIFICHE DELL'ASSICURAZIONE

Le eventuali modifiche dell'assicurazione devono essere provate per iscritto.

3.3. ALTRI CONTRATTI ASSICURATIVI

Il Contraente o l'Assicurato comunica per iscritto alla Compagnia l'esistenza e la successiva stipulazione di altri contratti assicurativi per lo stesso rischio. In caso di sinistro il Contraente o l'Assicurato deve darne avviso a tutti gli assicuratori, ai sensi dell'art. 1910 del Codice civile.

4. FORMA DELLE COMUNICAZIONI

Ogni comunicazione deve essere fatta in forma scritta, tramite e-mail all'Agenzia alla quale è assegnata la polizza: all'indirizzo polizza@wallife.it o tramite posta ordinaria all'indirizzo Wallife Insurance S.r.l. Via Vittorio Veneto 116, 00187 Roma. L'Agenzia alla quale è assegnata la polizza, predispone una apposita Area riservata nel proprio sito web cui il Contraente potrà accedere con proprie credenziali riservate, e dove effettuare direttamente le comunicazioni in merito alle polizze stipulate, compresa la denuncia di sinistro.

5. TITOLARITÀ DEI DIRITTI NASCENTI DALLA POLIZZA

Il Contraente esercita i diritti e le azioni nascenti dalla polizza.

Spetta in particolare al Contraente compiere gli atti necessari per la segnalazione del sinistro e l'accertamento e la liquidazione dei danni. Tale attività può essere svolta anche direttamente dall'assicurato, quando è diverso dal Contraente della polizza. La prestazione assicurativa dovuta a termini di polizza non può tuttavia essere erogata se non nei confronti dell'Assicurato, in quanto titolare dell'interesse alla copertura assicurativa.

6. TERMINE DI PRESCRIZIONE

I diritti derivanti dal presente contratto si prescrivono in due anni a norma dell'art. 2952 C.C.

7. CLAUSOLA DI INOPERATIVITÀ DELLA COPERTURA PER SANZIONI INTERNAZIONALI

UNIQA non è obbligata a garantire una copertura assicurativa e non è tenuta a pagare un Sinistro o a fornire una prestazione in applicazione di questo contratto se il fatto di garantire la copertura assicurativa, pagare il Sinistro o fornire la prestazione espone UNIQA a sanzioni, anche finanziarie o commerciali, divieti o restrizioni derivanti da risoluzioni delle Nazioni Unite, leggi o regolamenti dell'Unione Europea, degli Stati Uniti d'America, del Regno Unito o dell'Italia

8. LEGGE APPLICABILE E FORO COMPETENTE

Il contratto è disciplinato dalla Legge Italiana. Per le controversie relative al contratto il foro competente è esclusivamente quello della sede o del luogo di residenza o di domicilio del Contraente, dell'Assicurato, del Beneficiario o dei loro aventi diritto.



Quando e come devo pagare?

Il contratto prevede un premio annuo unitario per nucleo familiare assicurato dovuto dal Contraente per la copertura assicurativa di 12 mesi. Il Contraente alla sottoscrizione della polizza si impegna a corrispondere alla Compagnia di assicurazione, a titolo di premio, l'importo indicato nel Frontespizio di polizza.

9. CALCOLO DEL PREMIO

Il premio è dovuto per ciascun anno assicurativo, va pagato anticipatamente al fine di attivare la garanzia assicurativa, e tiene conto dei rischi assicurati e dei relativi massimali di copertura previsti dal contratto.

9.1. ONERI FISCALI

Il premio è comprensivo di imposte. Gli oneri fiscali relativi all'assicurazione, pertanto, sono a carico del Contraente, ma sono versati all'Erario direttamente dall'Assicuratore detraendoli dal premio pagato dal Contraente.

9.2. PAGAMENTO DEL PREMIO

Il pagamento del Premio della polizza avviene contestualmente all'acquisto della stessa a mezzo bonifico bancario, carte di credito o debito.



Quando comincia la copertura e quando finisce?

10. DURATA DELLA POLIZZA

La polizza ha validità annuale in base a quanto indicato nel contratto. Non è previsto il tacito rinnovo.

10.1. EFFICACIA ED EFFETTO DELLA COPERTURA

La copertura assicurativa viene attivata, conseguentemente all'accettazione della polizza ed al pagamento del premio.

L'assicurazione ha effetto dalle ore 24 del giorno in cui viene pagato il premio.



Come posso disdire la polizza?

11. DIRITTO DI RECESSO

Il Contratto non prevede diritto di recesso.

12. RISOLUZIONE DEL CONTRATTO

In caso di contraente persona fisica, la residenza del contraente deve essere nella Repubblica Italiana. In caso di spostamento della residenza in paese diverso dalla Repubblica Italiana, il contratto si risolve di diritto dalla data di spostamento e la Società rimborsa al contraente la parte di premio pagata e non goduta, senza le imposte.

In caso di mancata o tardiva comunicazione dello spostamento della residenza, la Società si riserva di chiedere al contraente il rimborso di ogni spesa eventualmente sostenuta.



A chi è rivolto questo prodotto?

Il prodotto è rivolto agli individui che vogliono proteggersi dai danni derivanti dal furto dell'identità digitale conservata negli Apparati digitali dell'Assicurato.

SEZIONE PERDITE PECUNIARIE

Le garanzie riportate nella presente sezione sono prestate da UNIQA VERSICHERUNG AG.



Che cosa è assicurato?

13. PROTEZIONE IDENTITÀ DIGITALE

L'assicurazione copre gli eventuali danni monetari sostenuti dall'Assicurato in conseguenza di un furto della propria identità digitale cui siano conseguiti eventi dannosi nell'ambito della vita privata e della vita professionale.

Sono coperti i seguenti eventi:

- a) **Accesso non autorizzato a conti correnti on-line, utilizzo fraudolento di carte di credito e sottrazione illecita di fondi;** la Compagnia si impegna, entro i limiti indicati in polizza, ad indennizzare l'assicurato del danno economico subito, a condizione che non abbia ricevuto alcun rimborso da parti terze, compresa l'istituzione finanziaria alla quale abbia richiesto il rimborso del medesimo ammontare di quanto sottratto illecitamente.
- b) **Furto di identità;** la copertura sarà operativa a condizione che l'Assicurato abbia provveduto a denunciare il furto alle Autorità competenti entro 24 ore da quando ne è venuto a conoscenza.
La Compagnia si impegna a rimborsare all'Assicurato i seguenti costi, entro i limiti indicati in polizza:
- il rimborso dei costi ragionevoli e necessari sostenuti dall'Assicurato per sottoporre nuovamente richieste di prestiti, finanziamenti o altre forme di credito che siano state respinte esclusivamente in ragione di un "Furto di Identità";
 - il rimborso dei costi ragionevoli e necessari sostenuti dall'Assicurato per la predisposizione di atti notori o altri documenti simili, ed altre spese connesse a questa necessità (es. chiamate telefoniche, spese di spedizione);
 - il rimborso del costo effettivo relativo alla sostituzione dei documenti (es. patenti di guida, passaporti, carta di Identità, certificati di matrimonio, certificati azionari) in ragione di un "Furto di Identità" (es. costo per ulteriori spese legali, dichiarazioni giurate);
 - Spese di viaggio (le spese di carburante, parcheggi, biglietti di aerei o treni, le spese di alloggio) necessarie per ottenere documenti sostitutivi a seguito di un "Furto di Identità".
- c) **Cyberbullismo, cyberstalking e danni alla reputazione online;** la Compagnia si impegna a rimborsare all'Assicurato, entro i limiti indicati in polizza:
- le spese necessarie per presentare istanza di oscuramento ai sensi di legge al titolare del trattamento o al gestore del sito internet o del social media per porre fine all'azione di diffamazione e/o cyber bullismo e/o cyber stalking nei confronti dell'Assicurato;
 - le spese necessarie per rivolgersi al Garante della Privacy se il titolare del trattamento o il gestore del sito internet o del social media non ha ottemperato all'oscuramento entro 48 ore dalla richiesta;
 - le spese necessarie per le prime 10 ore di supporto psicologico la cui necessità – certificata dal proprio medico curante – si potrebbe presentare in seguito alla diffamazione e/o al cyber bullismo e/o cyber stalking subito dall'assicurato;
 - In alternativa al pagamento di un indennizzo o delle spese, l'assicurato può richiedere l'intervento del Provider convenzionato con la Compagnia per le seguenti prestazioni:
 - Supporto alla richiesta di cancellazione delle informazioni in accordo col gestore del sito Web coinvolto o con la piattaforma di Social Media, con l'aiuto di un esperto di Digital Risk, entro 24 ore;
 - Monitoraggio online mediante scansione di siti Web delle informazioni sull'Assicurato disponibili al pubblico sul web e su dark web per la segnalazione di violazioni dei dati web dell'Assicurato e/o dei familiari (identità e dati finanziari) e per l'avviso via e-mail all'Assicurato di eventuali rischi identificati. Questo servizio sarà disponibile dalla data di denuncia del Sinistro per un periodo di 6 mesi.

Le spese per le prestazioni di cui al punto i e ii sono direttamente a carico della Compagnia fino all'eliminazione di massimo 10 link all'anno. Il Provider si impegna ad eseguire le attività di cui ai punti i e ii compiendo tutti gli sforzi necessari senza, tuttavia, poterne sempre garantire il risultato.

Sono escluse le prestazioni per consulenza o contenzioso legale e giudiziario.



Che cosa non è assicurato?

14. RISCHI ESCLUSI

In riferimento agli eventi di **accesso non autorizzato a conti correnti on-line, utilizzo fraudolento di carte di credito e sottrazione illecita di fondi**, la copertura assicurativa non opera nel caso in cui il danno economico sia:

- stato totalmente rimborsato dall'Istituzione finanziaria e, in caso di rimborso parziale, opera per la differenza;
- causato fraudolentemente dall'Assicurato o da persone che convivono con la persona assicurata;
- derivante dal pagamento di riscatti a scopo di estorsione o di pagamenti effettuati a titolo volontario (ad es. romance scam, trucco del nipote, ecc.);
- dovuto all'attivazione di abbonamenti (ad esempio canoni e contributi di adesione).

La Copertura, inoltre, non opera in caso di furto, perdita o smarrimento di carte di credito, carte di debito o carte prepagate, o di sinistri che abbiano causato la perdita di moneta virtuale (ec. Criptovalute, sistemi di pagamento in moneta virtuale).

Per eventi di **furto di identità**, la copertura non opera in caso di danni indiretti, quali ad esempio perdite di chance o di profitto.

Per gli eventi di **Cyber-bullismo, cyberstalking e danni alla reputazione online**, la copertura assicurativa non opera in caso di:

- cyber bullismo o danno alla reputazione online causato da una pubblicazione di materiale da parte di un familiare o altra persona che risiede normalmente con l'Assicurato;
- cyber bullismo già iniziato o danno alla reputazione online causato da una pubblicazione di materiale precedente all'inizio del periodo di assicurazione;
- danno reputazionale causato da una pubblicazione di materiale conforme ai fatti nel rispetto delle Leggi a tutela della Privacy;
- danno reputazionale dovuto alla registrazione a siti Web che hanno lo scopo di promuovere la violenza, contenuti pedopornografici, discriminatori o che non rispettino i diritti umani e civili e ogni altra promozione di contenuti e azioni che costituiscano reato;
- cyber bullismo o danno reputazionale causato da comunicazione scambiata tramite e-mail e/o chat istantanea in cui i contenuti non sono pubblicamente disponibili;
- cyber bullismo o danno reputazionale causato all'interno di chat room private, gruppi di notizie o altre aree protette da accessi non autorizzati;
- danno reputazionale a persona famosa, la cui vita e il cui comportamento sono al centro dell'interesse pubblico;
- danno reputazionale a persona che ricopra la carica di Amministratore di:
 - enti di beneficenza,
 - società con un fatturato superiore a 2 milioni di euro o con un bilancio superiore a 200 milioni di euro.

La copertura non opera, inoltre, in caso di danno alla reputazione della personalità quando questa sia:

- conseguenza di una provocazione da parte di una persona assicurata. Ciò vale anche se la persona assicurata ha in questo modo risposto a una precedente provocazione dell'autore degli attacchi;
- in relazione allo svolgimento di un'attività di natura politica o religiosa delle persone assicurate.



Ci sono limiti di copertura?

15. FRANCHIGIE, MASSIMALE E LIMITI DI INDENNIZZO/RIMBORSO

Qualunque rimborso corrisposto dalla Compagnia viene effettuato previa detrazione della franchigia prevista in polizza, per ogni singolo evento assicurato. La Compagnia non è tenuta a pagare una somma superiore a quanto effettivamente perduto dall'assicurato in conseguenza del sinistro e comunque non superiore ai limiti di rimborso (massimale), per ciascuna garanzia, riportati sul modulo di polizza.

Ad ogni sinistro il massimale viene progressivamente ridotto dell'importo pagato o stimato, con effetto immediato e fino al termine dell'anno assicurativo in corso. Detta progressiva riduzione non comporta comunque restituzione di premio.

15.1. RIEPILOGO DI FRANCHIGIE E LIMITI DI INDENNIZZO/RIMBORSO

Di seguito si riporta il riepilogo dei limiti di indennizzo/rimborso e delle franchigie previste dal contratto.

Copertura	Massimale	Franchigia / scoperto
Protezione identità digitale:	Fino a € 10.000 per sinistro e per anno assicurato	€350 per sinistro
<ul style="list-style-type: none"> • Accesso non autorizzato a conti correnti on-line, utilizzo fraudolento di carte di credito e sottrazione illecita di fondi; 		
<ul style="list-style-type: none"> • Furto di identità; 	Fino a 1.000€ per sinistro e per anno assicurato	
<ul style="list-style-type: none"> • Cyberbullismo, cyberstalking e danni alla reputazione online 	Fino a € 1.500 per sinistro e per anno o, in caso di utilizzo del servizio di cancellazione offerto dal partner convenzionato, eliminazione o deindicizzazione di 10 link	€150 per sinistro. In caso di accesso al servizio di cancellazione offerto dal partner convenzionato non verrà applicata alcuna franchigia



Dove vale la copertura?

16. EFFICACIA / VALIDITÀ TERRITORIALE DELL'ASSICURAZIONE

La copertura vale in tutto il mondo.



Che obblighi ho? Quali obblighi ha l'impresa

17. CHE COSA FARE IN CASO DI SINISTRO?

17.1. OBBLIGHI DELL'ASSICURATO – AVVISO DI SINISTRO - SERVIZIO DI CONTACT CENTER

L'Assicurato che subisce un sinistro a termini della presente polizza ne informa tempestivamente l'Assicuratore, non appena ne viene a conoscenza e comunque non oltre **TRE** giorni da quel momento. L'Assicurato in caso di sinistro deve altresì adottare tutte le misure ragionevoli e necessarie per ridurre al minimo i danni (es. bloccare conto o carta di credito), ivi comprese la denuncia alla Polizia Postale Italiana, ed alla Istituzione Finanziaria.

L'Assicurato deve inoltre procedere, nel più breve tempo possibile, con l'invio delle ulteriori indicazioni sulle modalità di accadimento del sinistro di cui egli sia venuto a conoscenza, nonché di eventuali documenti e/o atti relativi al sinistro successivamente a lui pervenuti.

L'Assicurato può denunciare il sinistro tramite:

- telefono, contattando la Centrale Operativa al numero +39 06 929 156 91 e fornendo ogni informazione richiesta o comunque ritenuta necessaria per la descrizione del sinistro avvenuto;
- posta ordinaria indirizzata a: Wallife Insurance – Ufficio Sinistri - Via Vittorio Veneto, 116 - 00186 Roma;
- posta elettronica indirizzata a: sinistri@wallife.it;
- posta elettronica certificata, solo per i titolari di Posta Elettronica Certificata (PEC) indirizzata a: wallifeinsurance@legalmail.it.

In assenza di comunicazione del sinistro la Compagnia non ha alcuna possibilità di procedere alla sua liquidazione.

L'Assicurato può richiedere informazioni sullo stato del sinistro da lui denunciato chiamando il numero +39 06 929 156 91.

In caso di denuncia tardiva del sinistro, e comunque oltre i **TRE** giorni dal momento della conoscenza del sinistro, la Compagnia di Assicurazione si riserva di non rispondere dei maggiori danni verificatisi rispetto al momento in cui l'assicurato ha avuto conoscenza del sinistro.

Su richiesta della Compagnia, l'Assicurato è tenuto a fornire qualsiasi documentazione in ordine alle modalità di accadimento del sinistro e del danno subito.

17.1.1. QUANDO SUBISCE UN TRASFERIMENTO ELETTRONICO NON AUTORIZZATO DI FONDI, L'ASSICURATO:

1. adotta tutte le misure ragionevoli per impedire ulteriori perdite economiche (es. contattare immediatamente l'Istituzione Finanziaria che ha emesso il Dispositivo di Accesso, o detiene il Conto dal quale sono stati effettuati i Trasferimenti non autorizzati; cambiare le credenziali di accesso al dispositivo o al conto; denunciare l'evento all'Autorità giudiziaria);
2. richiede il rimborso da parte dell'Istituzione Finanziaria della perdita economica sofferta;
3. invia una comunicazione, anche via e-mail, con le informazioni richieste dalla Compagnia ai fini dell'accertamento del danno economico subito;
4. fornisce qualsiasi altra informazione o documentazione pertinente al sinistro che la Compagnia potrà richiedere;
5. fornisce prova che un sistema di sicurezza valido di sua scelta o quello incluso nella nostra applicazione Wallife era installato, attivo e aggiornato nei dispositivi da lui utilizzati mentre leggeva l'e-mail di phishing o l'sms di smishing e avviava, eseguiva e autorizzava la transazione monetaria fraudolenta autorizzata a causa del phishing o dello smishing;
6. se ha optato per un sistema di sicurezza valido di sua scelta, fornisce le seguenti informazioni su di esso:
 - nome e versione;
 - prova di acquisto (se non si tratta di una versione gratuita);
 - contratto di licenza con l'utente finale;
 - documentazione del software con descrizione della protezione fornita;
7. fornisce qualsiasi registro o cronologia di attività - del sistema operativo o di altre fonti - disponibile nei dispositivi dell'utente e in grado di dimostrare che il sistema di sicurezza era installato, attivo e aggiornato quando l'utente ha letto l'e-mail di phishing o l'sms di smishing e ha avviato, eseguito e autorizzato la transazione monetaria fraudolenta autorizzata a causa del phishing o dello smishing.

17.1.2. QUANDO SUBISCE IL FURTO DI IDENTITÀ, L'ASSICURATO:

1. Invia, non più tardi di 90 giorni successivi alla scoperta da parte dell'Assicurato dal sinistro, la documentazione sul danno economico subito e fornisce le informazioni e/o la documentazione che dovesse essere richiesta;
2. adotta tutte le misure ragionevoli per mitigare o evitare le perdite risultanti dal Furto di identità;
3. fornisce tutta l'assistenza e la cooperazione che la Compagnia potrà richiedere per l'investigazione e la determinazione di eventuali perdite economiche.

17.1.3. QUANDO SUBISCE ATTI DI CYBERBULLISMO, CYBERSTALKING O DI LESIONE DELLA REPUTAZIONE, L'ASSICURATO:

1. richiede al gestore della pagina di rimuovere o oscurare il contenuto ritenuto offensivo o denigratorio;
2. qualora non fosse eliminato entro 24 ore, si rivolge al Garante della Privacy;
3. denuncia l'accaduto all'autorità di sicurezza pubblica.

In caso di richiesta di intervento del Provider convenzionato, il Contraente o l'Assicurato dovrà fornire un collegamento URL / schermata e quant'altro dell'evento, rilasciando all'assicuratore o a chi per suo conto interviene per eseguire le prestazioni assicurate i consensi e le autorizzazioni previsti dalla normativa in materia di tutela dei dati personali.

Quando si registra e si utilizza il servizio di monitoraggio online l'utente:

- a) deve avere almeno diciotto anni.
- b) deve seguire le regole sulla protezione dei dati.

Quando si registra e si utilizza il servizio di monitoraggio online per conto di un membro non minore della famiglia Assicurato:

- a) l'utente deve avere almeno diciotto anni;
- b) il familiare Assicurato deve autorizzare l'utente ad agire per conto suo e ad autorizzare l'utilizzo dei suoi dati;
- c) L'utente deve attenersi alle norme sulla protezione dei dati, specialmente se attiva il servizio per conto di un familiare;
- d) accettando di utilizzare il servizio, il familiare accetterà i presenti Termini e Condizioni;
- e) l'utente non ha nessun diritto di accesso alle informazioni relative al servizio di monitoraggio per conto del familiare.

17.2. PAGAMENTO DELL'INDENNIZZO PER LE GARANZIE PRESTATE NELLA SEZIONE PERDITE PECUNIARIE CHE PREVEDANO IL RIMBORSO ALL'ASSICURATO

L'Assicuratore, ricevuta la necessaria documentazione, verificata l'operatività della garanzia, determinato l'indennizzo dovuto ed identificato il beneficiario dello stesso, ove previsto, provvede entro 30 giorni al pagamento.

17.3. INOSSERVANZA DEGLI OBBLIGHI RELATIVI AI SINISTRI

Il Contraente è responsabile verso la Compagnia di ogni pregiudizio derivante dall'inosservanza dei termini o degli altri obblighi di cui ai punti "OBBLIGHI DELL'ASSICURATO – AVVISO DI SINISTRO - SERVIZIO DI CONTACT CENTER".

17.4. ESAGERAZIONE DOLOSA DEL DANNO

Il Contraente o l'Assicurato che esagerano l'entità del danno e adoperano a giustificazione mezzi o documenti menzogneri o fraudolenti, alterano le tracce del sinistro o facilitano il progresso di questo, perdono il diritto all'indennizzo.

17.5. VALUTA DEI PAGAMENTI

Le indennità ed i rimborsi vengono corrisposti in Italia in Euro. Nel caso di spese sostenute in Paesi non appartenenti all'Unione Europea, il rimborso verrà calcolato al cambio rilevato dalla Banca Centrale Europea, relativo al giorno in cui l'Assicurato ha sostenuto le spese.

ALLEGATO 1**INFORMATIVA PRIVACY
ai sensi dell'art. 13 del Regolamento Europeo 2016/679 (GDPR)**

I dati personali forniti dal cliente all'atto della sottoscrizione della presente informativa saranno trattati da Wallife nel rispetto della normativa vigente in materia di protezione dei dati personali e dei principi di correttezza, liceità, trasparenza e tutela della riservatezza da essa previsti.

TITOLARE DEL TRATTAMENTO

1. Il Titolare del trattamento dei dati per l'attività di intermediazione e distribuzione assicurativa effettuata è Wallife Insurance s.r.l. (società del Gruppo Wallife SpA), agente di assicurazione iscritto al RUI conservato presso Ivass n. A000710058, con sede legale in Roma, via Vittorio Veneto n. 116 c.a.p. 00187, P.IVA 15766131005.
2. Wallife, in qualità di Titolare del trattamento, può nominare, per ciascuna delle attività sociali svolte e quando ciò sia richiesto dalla normativa, responsabili del Trattamento ovvero incaricati appositamente individuati. Il titolare può essere contattato all'indirizzo e-mail info@wallife.com
3. Soggetto destinatario del trattamento è la Compagnia di assicurazione che presta la garanzia prevista nella polizza distribuita da Wallife e che, per tale ragione, entra in contatto con i dati personali degli interessati raccolti dall'intermediario nell'esecuzione del mandato di agenzia conferito.

BASE GIURIDICA DEL TRATTAMENTO

1. La base giuridica del trattamento dei dati effettuati da Wallife per le finalità specificate nella presente informativa, ai sensi dell'art. 6 Gdpr, è l'esecuzione del contratto assicurativo intermediato dal Titolare e di cui il soggetto interessato è parte ovvero a cui il soggetto aderisce nel caso in cui il contratto sia sottoscritto in modalità collettiva, in tal caso i dati dell'interessato si intendono raccolti presso terzi.

TIPOLOGIA DI DATI RACCOLTI E MODALITA' DI RACCOLTA

1. I dati personali raccolti dal Titolare sono quelli forniti dal soggetto interessato, e sono ad esempio: nome, cognome, data di nascita, codice fiscale, documento identificativo, identità di genere, indirizzo e-mail, recapito telefonico, città, codice di avviamento postale, nazione, estremi di carta di credito ovvero ogni ulteriore dato che Wallife dovesse ritenere necessario, ai sensi e nel rispetto della normativa Gdpr, per l'efficace espletamento delle finalità di trattamento di cui alla presente informativa.
2. Il Titolare informa inoltre che ha facoltà di raccogliere altresì i c.d. dati di utilizzo ovvero le informazioni raccolte in modo automatico dal sito internet e dall'applicazione scaricabile sui device . ovvero da applicazioni di parti terze connesse ed integrate dalla app di Wallife (es. indirizzi IP, caratteristiche del browser utilizzato, dettagli temporali dell'accesso e della richiesta di attivazione della garanzia ecc.).

DATI RACCOLTI PRESSO SOGGETTI TERZI

1. Nel caso in cui i dati dell'interessato non siano raccolti presso l'utente stesso ma presso soggetti terzi (es. polizza di assicurazione collettiva) Wallife, in qualità di Titolare del trattamento, fornisce all'interessato tutte le informazioni previste all'interno della presente informativa e contenente i propri dati e quelli del responsabile del trattamento, ove incaricato, la base giuridica, le modalità con cui viene effettuato il trattamento e le finalità per le quali lo stesso viene posto in essere.
2. Wallife comunica al soggetto interessato la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.
3. Nel caso in cui la raccolta dei dati dell'interessato avvenga presso terzi, l'utente ha sempre diritto di chiedere la correzione dei propri dati qualora gli stessi fossero stati comunicati dai terzi ovvero raccolti da Wallife in modo inesatto.

MODALITA' DEL TRATTAMENTO

1. Wallife, in qualità di titolare, tratta i dati personali con l'ausilio di strumenti informatici e/o telematici e, in ogni caso, nel rispetto di ogni misura cautelativa che ne garantisca la sicurezza e la riservatezza per il tempo necessario allo svolgimento del servizio richiesto dal soggetto interessato ovvero dalle finalità del contratto e del trattamento descritti nella presente informativa. L'interessato può sempre richiedere l'interruzione del trattamento e/o la cancellazione dei dati trattati.
2. Il trattamento dei dati personali conferiti verrà effettuato a mezzo di soggetti espressamente designati dal Titolare con apposite nomine che trattano i dati in qualità di responsabili ovvero di soggetti incaricati espressamente autorizzati. Oltre al Titolare ed ai soggetti da esso nominati possono avere accesso ai dati anche i soggetti incaricati coinvolti nella gestione del sito internet di Wallife (personale amministrativo, commerciale, marketing, legali, amministratori di sistema) ovvero soggetti esterni (fornitori di servizi tecnici, provider, amministratori di sistema).
3. I dati personali sono trattati presso le sedi operative del Titolare, del responsabile ovvero in ogni altro luogo in cui le parti coinvolte nel trattamento siano localizzate, ivi compresi stati appartenenti all'Unione Europea.

CONSERVAZIONE DEI DATI

1. I dati sono conservati da Wallife per il tempo necessario allo svolgimento delle attività concordate nel contratto ed

all'espletamento delle attività costituenti le finalità per cui sono stati raccolti.

2. In qualsiasi momento il soggetto interessato ha diritto di chiedere a Wallife l'interruzione del trattamento e la cancellazione dei propri dati, resta inteso che gli stessi dovranno essere conservati da Wallife in ogni caso per il tempo necessario all'adempimento di obblighi di legge, regolamentari ovvero delle disposizioni impartite da Autorità di vigilanza e controllo di settore.
3. Al termine del periodo di conservazione i dati conferiti saranno cancellati sia dai data base di Wallife Insurance s.r.l. che dalla eventuale conservazione cartacea, se esistente.

FINALITA' DEL TRATTAMENTO DEI DATI RACCOLTI

1. Il trattamento dei dati sarà finalizzato allo svolgimento delle attività di seguito elencate:
 - a) Distribuzione e gestione di contratti di assicurazione proposti all'interno del sito e dell'applicazione la cui garanzia viene prestata dalla Compagnia di assicurazione di volta in volta impegnata a garantire il rischio portato dalla polizza intermediata da Wallife Insurance e specificamente nella informativa allegata al contratto di assicurazione, rinvenibile anche nel sito wallife.it (consenso obbligatorio);
 - b) svolgimento, previo espresso consenso dell'interessato, di attività di marketing diretto, quali l'invio, tramite e-mail, SMS ovvero MMS, di materiale pubblicitario e di comunicazioni aventi contenuto informativo e/o promozionale in relazione a prodotti o servizi forniti e/o promossi da Wallife o da suoi partner commerciali (consenso facoltativo);
 - c) svolgimento, previo espresso consenso, di attività di profilazione individuale o aggregata e di ricerche di mercato volte, ad esempio, all'analisi delle abitudini e delle scelte di consumo, all'elaborazione di statistiche sulle stesse o alla valutazione del grado di soddisfazione rispetto ai prodotti ed ai servizi proposti.

DIRITTI DEGLI INTERESSATI

1. I soggetti cui si riferiscono i dati personali trattati da Wallife ovvero dai Responsabili nominati possono in ogni momento esercitare i diritti loro riconosciuti ai sensi del Regolamento europeo 679/2016 (GDPR) e della normativa nazionale e, precisamente, possono:
 - a) Revocare il consenso prestato in precedenza al trattamento dei propri dati personali;
 - b) Opporsi al trattamento dei dati che lo riguardano quando ciò venga effettuato su base giuridica differente rispetto a quella per cui l'interessato ha prestato il proprio consenso;
 - c) Avere conferma dell'esistenza o meno, presso il Titolare, di dati personali che li riguardano, anche se non ancora registrati, ed esercitare il relativo diritto di accesso per conoscere tutti gli aspetti connessi al trattamento effettuato dal Titolare;
 - d) Chiedere la rettifica dei dati personali inesatti ovvero l'integrazione quando siano stati richiesti ovvero acquisiti in modo incompleto;
 - e) Chiedere la limitazione del trattamento per il tempo necessario al Titolare ad effettuare le verifiche di legge nel caso in cui l'interessato abbia contestato l'esattezza dei propri dati, formulato opposizione al trattamento ovvero richiesto la cancellazione degli stessi per illiceità del trattamento o nel caso in cui gli stessi siano necessari all'interessato per l'accertamento, l'esercizio ovvero la difesa di un diritto in sede giudiziaria;
 - f) ricevere i dati in formato strutturata e leggibile da un dispositivo automatico e trasmetterli ad altro titolare senza impedimenti da parte di Wallife (portabilità dei dati);
2. Nel caso in cui il soggetto interessato ritenga che il trattamento dei propri dati sia effettuato in violazione di legge, può proporre reclamo ai sensi dell'art. 77 Gdpr all'autorità di controllo dello stato nel quale risiede abitualmente, lavora ovvero del luogo ove si è verificata la presunta violazione.

COOKIES

1. Il sito internet e l'applicazione da scaricare sul device dell'utente di Wallife utilizzano cookies ovvero strumenti di tracciamento che, in caso di consenso prestato da parte dell'interessato, consentono al Titolare di raccogliere e salvare informazioni sul dispositivo dell'Utente mentre questo utilizza l'applicazione o il sito internet.

COMUNICAZIONI DEI DATI A TERZI

1. Il Titolare del trattamento ha facoltà di trasmettere a terzi i dati del soggetto interessato raccolti per adempiere obblighi di legge cui Wallife è soggetta sia ai fini di vigilanza e controllo che fiscali, ed ogni altro incombente sulla medesima gravante anche nei confronti di autorità di pubblica sicurezza (es. Richieste avanzate dall'Autorità di Vigilanza Ivass, dall'Autorità garante per la protezione dei dati ovvero Agenzie delle entrate).

ULTERIORI INFORMAZIONI SUL TRATTAMENTO

1. Nello svolgimento delle attività di cui alla presente informativa, il Titolare utilizza software e servizi che consentono a Wallife di monitorare ed analizzare i dati di navigazione idoneo a tenere traccia del comportamento e delle ricerche effettuate dall'utente.
2. I dati personali raccolti e trattati dal Titolare possono essere utilizzati da questo in procedimenti giudiziari ovvero nelle fasi antecedenti per articolazione della difesa; a tale riguardo, l'utente dà atto e dichiara di essere consapevole che il Titolare possa essere obbligato da autorità pubbliche alla comunicazione di tali dati.