

1 Disposizioni generali

Le presenti « Condizioni dell'offerta opzioni Security» si applicano ai servizi di Internet Security, Identity Security e Secure Internet Traffic (di seguito «Servizio») di Swisscom (Svizzera) SA (di seguito «Swisscom»). Queste Condizioni sono valide a integrazione delle disposizioni contrattuali già in essere tra il cliente e Swisscom, in particolare le «Condizioni generali di contratto Swisscom per i clienti commerciali» («CGC»), consultabili all'indirizzo www.swisscom.ch/b2b-legal.

2 Servizi di Swisscom

2.1 Aspetti generali

È possibile abbonarsi a singoli servizi oppure combinandoli in base alle proprie preferenze.

2.2 Gamma dei servizi di Internet Security

Il servizio Internet Security viene proposto sotto forma di un abbonamento che consente di proteggere fino a dieci dispositivi (cfr. <https://www.swisscom.ch/pmi-security>).

I filtri applicati sulla rete, ad esempio in funzione antispam e antivirus, sono di pertinenza del fornitore di Internet o di e-mail.

Su Windows, Internet Security comprende i seguenti funzionalità:

- Internet Security offre una protezione, mediante il proprio firewall o in combinazione con le funzioni di firewall del sistema operativo Windows, da attacchi provenienti da Internet e con i quali soggetti non autorizzati cercano di accedere a dati e/o programmi del cliente.
- Internet Security protegge da programmi nocivi come virus, spyware, worm, trojan e rootkit con i quali soggetti non autorizzati cercano di danneggiare o usare in modo improprio dati e/o programmi del cliente.
- Internet Security consente limitazioni dell'accesso di singoli utenti a Internet attraverso il blocco (protetto da password o basato sul profilo) di determinati siti, la gestione di whitelist e blacklist per consentire o

«Condizioni dell'offerta opzioni Security»

per clienti commerciali

bloccare l'accesso ai siti e l'inserimento degli orari di navigazione consentiti.

Su Mac, Internet Security comprende i seguenti funzionalità:

- Internet Security protegge da virus, worm e altri programmi nocivi.
- Internet Security rimuove il software installato di nascosto sul computer del cliente.
- Internet Security consente limitazioni dell'accesso di singoli utenti a Internet attraverso il blocco (protetto da password o basato sul profilo) di determinati siti, la gestione di whitelist e blacklist per consentire o bloccare l'accesso ai siti e l'inserimento degli orari di navigazione consentiti.

Su Android (smartphone e tablet), Internet Security comprende i seguenti funzionalità:

- Internet Security protegge da virus, worm e altri programmi nocivi.
- Internet Security identifica i siti non sicuri.
- Internet Security consente di limitare l'accesso di singoli utenti a siti indesiderati, con l'aiuto della protezione del browser. Inoltre, mediante un sistema configurabile di gestione delle applicazioni è possibile bloccare alcuni programmi (app).
- Internet Security offre un'ampia sicurezza antifurto e consente di bloccare o resettare il dispositivo Android con accesso remoto, nonché di riprodurre un segnale acustico di allarme sul dispositivo rubato o smarrito.

Su iOS (iPhone e iPad), Internet Security comprende i seguenti funzionalità:

- Internet Security identifica i siti non sicuri e offre protezione nel banking online e nello shopping online.
- Internet Security consente limitazioni dell'accesso di singoli utenti a Internet attraverso il blocco (protetto da password o basato sul profilo) di determinati siti, la gestione di whitelist e blacklist per consentire o bloccare l'accesso ai siti e l'inserimento degli orari di navigazione consentiti.

Una licenza Internet Security può essere utilizzata in qualsiasi momento per un altro dispositivo.

Una panoramica aggiornata e dettagli sulle diverse funzionalità sono disponibili sul sito <https://www.swisscom.ch/pmi-security>.

2.3 Gamma dei servizi di Identity Security

Identity Security tutela dal furto di dati e protegge l'identità digitale dalla criminalità informatica.

- È possibile monitorare le attività sospette di fino a un massimo di dieci indirizzi.
- I dati personali collegati agli indirizzi e-mail (ad es. indirizzo e-mail, nome utente, password, numero ID, numero di carta di credito) sono monitorati in modo permanente.
- In caso di furto o impiego abusivo dei dati connessi all'indirizzo e-mail, il cliente viene allertato in forma proattiva e riceve immediatamente istruzioni per limitare i danni.
- Un manager di password memorizza le password in forma sicura all'interno di una cassaforte virtuale, con funzione di sincronizzazione per tutti i dispositivi
- Il manager di password aiuta anche a creare password forti. Ora è necessaria una sola password master.

Una licenza Identity Security può essere utilizzata in qualsiasi momento per un altro indirizzo e-mail o numero di carta di credito cancellando nell'app un indirizzo e-mail o numero di carta di credito esistente.

2.4 Gamma dei servizi di Secure Internet Traffic

Secure Internet Traffic permette al cliente di utilizzare una soluzione di sicurezza basata su software della ditta Zscaler Inc. (con sede in California, di seguito denominata «Zscaler»). Il cliente acquista una licenza per ogni terminale da proteggere e installa la relativa applicazione sul dispositivo. Il servizio è fornito come soluzione cloud nel percorso standard del traffico Internet e analizza il traffico web (contenuti) dell'utente in entrata e in uscita per individuare varie tipologie di minacce. Anche il traffico web con cifratura https dell'utente viene codificato a questo fine nella soluzione cloud di Zscaler e quindi decodificato al termine

«Condizioni dell'offerta opzioni Security»

per clienti commerciali

dell'analisi. Per individuare le minacce e attuare la protezione si utilizzano diverse tecniche di sicurezza.

Una licenza Secure Internet Traffic può essere utilizzata in qualsiasi momento per un altro utente. La gestione delle licenze è affidata al cliente stesso tramite My Swisscom Business.

2.5 Gamma delle prestazioni Mail Security

Mail Security filtra le e-mail del cliente in entrata e in uscita e protegge da numerose minacce. Oltre al rilevamento di spam e virus, l'Advanced Threat Protection (ATP) offre una protezione contro minacce mirate e altamente complesse, come ransomware, attacchi misti e mirati e attacchi di phishing. Per individuare le e-mail pericolose, ATP utilizza il sandboxing, motori di analisi forense innovativi, la riscrittura e la scansione di URL. In caso di rilevamento di attacchi, l'utente ne viene informato in tempo reale.

Per l'individuazione di queste minacce si utilizza una combinazione di procedimenti tecnici, di motori di scansione basati su firme e procedure euristiche.

Mail Security protegge automaticamente tutti gli indirizzi e-mail di un dominio da indicare durante l'ordine. La protezione di singoli indirizzi e-mail di un dominio non è possibile. Non è nemmeno possibile escludere dalla protezione singoli indirizzi e-mail.

2.6 Aggiornamenti (update)

Con Internet Security, i componenti dei servizi necessari per l'individuazione di virus e di altri programmi nocivi sono costantemente soggetti ad aggiornamento automatico, al fine di adeguare le funzionalità di protezione alle nuove minacce identificate, a fronte di limitazioni minime all'utilizzo dei servizi online.

Identity Security necessita di aggiornamenti dell'applicazione, i quali sono indipendenti dal sistema di individuazione e di allarme dei dati privati divulgati o sottratti.

Anche Secure Internet Traffic necessita di aggiornamenti dell'applicazione. L'applicazione nel cloud, che si occupa della verifica dei dati, viene costantemente aggiornata in modo automatico e senza limitazioni della funzionalità.

Mail Security non necessita di un'applicazione installata dal cliente. L'applicazione nel cloud, che si occupa della verifica dei dati, viene costantemente aggiornata in modo automatico e senza limitazioni della funzionalità.

Nuove versioni del software sono messe a disposizione del cliente a titolo gratuito.

2.7 Comunicazione del guasto e supporto

Se si verificano guasti alle funzionalità di base dei servizi, il cliente può avvalersi del supporto gratuito dell'helpdesk di Swisscom.

In caso di problemi connessi ai terminali e all'infrastruttura privata, sono disponibili unità di assistenza (a pagamento).

3 Prestazioni e obblighi del cliente

3.1 Requisiti di utilizzo generali

Internet Security & Identity Security

L'abbonamento ai servizi presuppone un abbonamento alla rete fissa o mobile di Swisscom e l'attivazione dell'accesso a My Swisscom Business.

Secure Internet Traffic & Mail Security

L'abbonamento ai servizi presuppone un abbonamento "inOne PMI office" presso Swisscom e l'attivazione dell'accesso a My Swisscom Business.

3.2 Requisiti di sistema e aggiornamenti

L'utilizzo del software presuppone che il relativo terminale soddisfi i requisiti di sistema. Una panoramica costantemente aggiornata dei requisiti di sistema è pubblicata sul portale Swisscom (<https://www.swisscom.ch/pmi-security>).

L'utilizzo dell'intera gamma di prestazioni del relativo servizio richiede che il cliente, per l'intera durata dell'abbonamento, provveda a installare tutti gli update, usi la versione aggiornata del software, utilizzi un sistema operativo conforme ai requisiti di sistema correnti e lo tenga costantemente aggiornato.

Per l'installazione di una nuova versione del software il cliente può decidere autonomamente il momento dell'installazione, con riserva di ripercussioni sulla gamma dei servizi. Una nuova

«Condizioni dell'offerta opzioni Security»

per clienti commerciali

versione del software può includere la modifica ai requisiti di sistema. Il cliente si impegna a tenersi periodicamente informato sui requisiti di sistema.

3.3 Download del software

Per avvalersi dei servizi, in alcuni casi è necessario installare un software dell'azienda F-Secure (Internet Security) o Zscaler (Secure Internet Traffic).

Al momento dell'attivazione del software, il cliente stipula direttamente con il produttore del software in questione un contratto di licenza che disciplina soprattutto le questioni tecniche relative alla gestione del software e al trattamento dei dati da parte del produttore.

Laddove ciò sia necessario, il cliente è responsabile del download del software, dei necessari componenti hardware e software e delle configurazioni dei computer.

3.4 Ripercussioni su altri tipi di servizi online

Il cliente accetta che, in conseguenza dell'impiego dei servizi Swisscom con i relativi parametri di sicurezza, alcuni servizi online non possano essere utilizzati oppure lo si possa fare solo in forma limitata.

4 Prezzi/fatturazione

4.1 Prezzi

I prezzi e i canoni di Swisscom applicati sono quelli aggiornati pubblicati su www.swisscom.ch/pmi-security o nella pagina del prodotto dell'abbonamento alla rete fissa o mobile.

I servizi elencati qui vengono fatturati pro rata temporis. Fanno eccezione in Mail Security gli indirizzi e-mail eccedenti il pacchetto base. Questi vengono sempre fatturati per il mese intero. Il giorno di riferimento è il 27 del mese. Al giorno di riferimento viene fatturato il numero massimo di indirizzi e-mail del mese di un dominio.

4.2 Fatturazione

Tutti i servizi qui descritti vengono addebitati mensilmente sulla fattura Swisscom del cliente.

Salvo accordi diversi, l'obbligo di pagamento decorre a partire dalla data di attivazione del servizio nell' My

Swisscom Business o negli altri sistemi di ordinazione di Swisscom.

4.3 Ritardo nel pagamento

Se entro il termine di scadenza il cliente non ha pagato la fattura, né presentato obiezioni motivate e per iscritto a tal proposito, è immediatamente in stato di mora. In aggiunta alle altre conseguenze della mora definite contrattualmente e giuridicamente, Swisscom ha la facoltà (nei limiti consentiti dalla legge) di interrompere la fornitura di tutti i servizi, di adottare ulteriori misure per prevenire l'ampliamento dei danni e/o di rescindere il contratto senza preavviso e senza indennizzo.

5 Proprietà intellettuale

Per tutta la durata del contratto, il cliente riceve il diritto, non trasferibile e non esclusivo, di utilizzare i servizi cui si è abbonato. Tutti i diritti di proprietà intellettuale, già esistenti o che dovessero insorgere durante l'adempimento del contratto, che appartengono a Swisscom o a soggetti terzi autorizzati, resteranno a Swisscom o ai soggetti terzi autorizzati. Se il cliente viola i diritti di beni immateriali di terzi e per questo viene chiamata in causa Swisscom, il cliente dovrà risarcire Swisscom.

6 Condizioni di licenza dei produttori di software; Rilevazione, trattamento e memorizzazione dei dati

6.1 Condizioni di licenza dei produttori di software

Nel quadro dei servizi descritti, la prestazione di Swisscom consiste principalmente nel conferire il diritto di utilizzare i servizi dei produttori di software per il software impiegato in base alle loro condizioni. Swisscom assicura di essere autorizzata a conferire al cliente i diritti concordati contrattualmente e garantisce che il servizio dei rispettivi produttori di software con le relative funzioni sia a disposizione, per il periodo di durata del contratto, secondo quanto previsto dalle specifiche del relativo produttore. Nel caso di lacune segnalate dal cliente immediatamente dopo averle riscontrate, Swisscom chiederà al produttore di software di rimuoverle entro un periodo adeguato.

«Condizioni dell'offerta opzioni Security»

per clienti commerciali

Laddove ciò non vada a buon fine il cliente, trascorso inutilmente un ulteriore periodo di tolleranza, in presenza di difetti di minore entità potrà richiedere a Swisscom un'adeguata riduzione del prezzo, mentre in presenza di gravi lacune potrà disdire il contratto in via straordinaria (ex nunc) e richiedere un rimborso pro rata delle prestazioni già versate. Non sono previsti ulteriori diritti del cliente.

Nell'ambito delle disposizioni di licenza del produttore del software hanno validità gli ulteriori documenti specificati da quest'ultimo che il cliente dichiara di accettare direttamente nei confronti del rispettivo produttore.

Eventuali trasferimenti di dati tra il cliente e il rispettivo produttore di software basati sull'utilizzo dei suoi software/delle sue prestazioni non sono oggetto del presente accordo e Swisscom non si assume alcuna responsabilità in proposito. Per quanto riguarda tali trasmissioni di dati, il relativo produttore di software non è sub-responsabile del trattamento di dati o ausiliario di Swisscom. Si applicano le relative regolamentazioni sulla protezione dei dati del produttore, cui si fa riferimento nella EULA o in altri documenti correlati (riportati di seguito). Spetta esclusivamente al cliente valutare la legittimità e l'idoneità di questi trasferimenti di dati per le proprie finalità ed eventualmente limitarli mediante misure tecniche o impostazioni specifiche del prodotto. Tale regolamentazione vale anche in un eventuale caso di supporto con l'assistenza di Swisscom, in cui Swisscom, in rappresentanza del cliente, concede eventualmente al produttore del software l'accesso ai dati del cliente.

6.2 Internet Security e Identity Security

L'EULA di F-Secure (<https://www.f-secure.com/de/legal/terms>), che il cliente accetta direttamente nei confronti di F-Secure, si applica anche nell'ambito della licenza.

Il modo in cui F-Secure tratta i dati è riportato, per Internet Security, nella «Direttiva sulla protezione dei dati per F-Secure Internet Security» (<https://www.f-secure.com/it/legal/privacy/consumer/total>), mentre per Identity Protection nella «Direttiva sulla protezione

dei dati per Identity Protection» (<https://www.f-secure.com/it/legal/privacy/consumer/id-protection>).

6.3 Secure Internet Traffic

L'EULA di ZScaler (<https://www.zscaler.com/legal/end-user-subscription-agreement>), che il cliente accetta direttamente nei confronti di F-Secure, si applica anche nell'ambito della licenza.

Nel quadro del presente accordo, la funzione di Swisscom consiste principalmente nel conferire il diritto di utilizzare i servizi di ZScaler. Swisscom assicura di avere l'autorizzazione per concedere al cliente i diritti concordati contrattualmente e garantisce che il servizio di ZScaler con le relative funzioni sia a disposizione, per il periodo di durata del contratto, secondo quanto previsto dalle specifiche di ZScaler. Nel caso di lacune immediatamente segnalate dal cliente dopo averle riscontrate, Swisscom chiederà a ZScaler di rimuoverle entro un periodo adeguato. Laddove ciò non vada a buon fine il cliente, dopo la scadenza di un ulteriore periodo di tolleranza, in presenza di difetti di minore entità potrà richiedere a Swisscom un'adeguata riduzione del prezzo, mentre in presenza di gravi lacune potrà disdire il contratto in via straordinaria (ex nunc) e richiedere un rimborso pro rata delle prestazioni già versate. Non sono previsti ulteriori diritti del cliente.

Eventuali trasferimenti di dati tra il cliente e ZScaler sulla base dell'utilizzo dei servizi di ZScaler non sono oggetto del presente accordo e Swisscom non si assume alcuna responsabilità in proposito. Si applicano le regolamentazioni sulla protezione dei dati di ZScaler, cui si fa riferimento nella EULA, negli altri documenti correlati e sul sito Internet di ZScaler (<https://www.zscaler.com/privacy/overview>). Spetta al cliente valutare la legittimità e l'idoneità di questi trasferimenti dei dati per le proprie finalità ed eventualmente limitarli mediante misure tecniche o impostazioni specifiche del prodotto.

In aggiunta, il cliente prende atto e accetta che, a seguito dell'utilizzo di Secure Internet Traffic, l'elaborazione del suo traffico dati su Internet (in particolare la decodifica, l'analisi dei contenuti, la ricodifica e l'inoltro o la sospensione del traffico di dati) vengono operate da ZScaler all'estero, ove non vige segreto delle telecomunicazioni. Nell'ambito dell'utilizzo di Secure Internet Traffic, il cliente

«Condizioni dell'offerta opzioni Security»

per clienti commerciali

rinuncia quindi consapevolmente al segreto delle telecomunicazioni e si assume la responsabilità di informarne preventivamente e in modo adeguato tutti gli utenti cui rende accessibile questo servizio.

6.4 Mail Security

Il servizio Mail Security viene fornito in data center geo-ridondanti in Svizzera, in collaborazione con un partner tecnologico con sede in Germania (nell'UE/nel SEE).

Conservazione fisica dei dati: i dati di log del servizio Mail Security si trovano in data center ubicati in Svizzera. Le e-mail in entrata e in uscita vengono memorizzate solo temporaneamente sulla piattaforma Mail Security finché non potranno essere consegnate al rispettivo mail server, dopodiché vengono cancellate. I dati di log provenienti dalle attività filtro sulle e-mail vengono salvati per dodici mesi, dopodiché vengono automaticamente cancellati.

Il trattamento automatico dei dati comprende i metadati della trasmissione di messaggi (indirizzo e-mail del mittente e del destinatario, oggetto, data/ora dell'ingresso e della consegna delle mail, indirizzi IP dei server interessati dalla comunicazione, codice errore e testo SMTP), il contenuto di e-mail e la classificazione delle mail (clean, spam, virus, infomail). Il trattamento dei dati avviene sul proprio hardware, ubicato nei centri di calcolo Swisscom (colocation). Non è previsto l'inoltro di altri dati (intestazione della mail, mittente, destinatario, oggetto, data, contenuto del testo) a terzi. Oltre al mandatario e ai rappresentanti designati del committente, non vi sono terzi che abbiano accesso ai dati. Nell'utilizzo della Advanced Threat Protection (Sandbox) il cliente acconsente a che i dati da analizzare siano trasmessi all'infrastruttura del produttore dell'applicazione con sede nel SEE.

In casi di supporto, il 3rd Level Support del produttore dell'applicazione ha accesso dall'estero ai dati dell'applicazione. L'accesso viene attivato da Swisscom in modo selettivo e mirato (casi di supporto e release). L'accesso avviene esclusivamente per l'adempimento del contratto. Per l'individuazione di spam e malware, il servizio Mail Security scambia metadati e dati sul contenuto delle e-mail con il sistema centrale del produttore

dell'applicazione con sede all'estero. Con l'utilizzo del servizio il cliente acconsente a tale trattamento.

Per l'analisi di problemi può essere necessario consentire a Swisscom l'accesso ai file log del cliente. Qualora Swisscom non sia in grado di risolvere personalmente il problema, è autorizzata a mettere i dati di servizio del cliente, necessari per l'analisi del problema, a disposizione del produttore dell'applicazione con sede all'estero (tramite un canale criptato).

7 Garanzia legale

Con i loro rispettivi servizi, Swisscom e il produttore di software garantiscono la sicurezza, ciascuno in base allo stato aggiornato della tecnica e nel quadro della gamma dei servizi offerti (cfr. punti da 2.2 a 2.5), a seconda del servizio acquistato o del sistema operativo.

Swisscom si impegna a garantire un'elevata disponibilità dei propri servizi. A integrazione delle disposizioni contrattuali esistenti tra Swisscom e il cliente, **Swisscom non fornisce però alcuna garanzia che le singole funzioni di protezione (cfr. punti da 2.2 a 2.5) assicurino una tutela assoluta. In particolare, Swisscom non garantisce che i servizi identifichino o prevengano ogni evento dannoso.**

Inoltre, Swisscom non fornisce garanzia

- per il funzionamento privo di interruzioni e di guasti, per la qualità e la costante disponibilità dei servizi e delle loro singole funzionalità;
- per il perfetto funzionamento dei servizi su tutti i terminali e in combinazione con tutti i componenti hardware e software, nonché i sistemi operativi;
- che attacchi, accessi di terzi o programmi nocivi non compromettano l'utilizzo di altri tipi di servizi e non danneggino in altro modo il cliente;
- per la funzionalità dei servizi su dispositivi che non sono stati acquistati presso Swisscom o che non sono riportati sulla lista dei dispositivi supportati.

8 Responsabilità

Swisscom non si assume alcuna responsabilità,

«Condizioni dell'offerta opzioni Security»

per clienti commerciali

- se nonostante il software installato e aggiornato si verificano danni sull'apparecchio protetto o sono accessibili siti indesiderati;
- se Identity Security non identifica un evento dannoso e ne consegue un danno.
- nel caso in cui Mail Security non individui un evento dannoso e ne consegua un danno.

Nel quadro di quanto consentito dalla legge, Swisscom respinge qualsiasi responsabilità, ad esempio per danni sotto forma di perdita di dati, smarrimento di password, mancati guadagni o conseguenze indirette.

Non risponde altresì di danni causati da un utilizzo dei propri servizi in modo contrario alla legge o alle norme del contratto.

Swisscom non risponde nel caso in cui la fornitura del servizio venga limitata o resa impossibile, parzialmente o del tutto, per cause di forza maggiore. Per forza maggiore si intende in particolare un caso di interruzione di corrente o la presenza di software dannosi (ad es. infezione da virus).

9 Durata e disdetta; promozioni

9.1 Durata e disdetta

I servizi possono essere disdetti da ciascuna delle parti in qualsiasi momento. Per i prodotti Security qui descritti non è prevista una durata contrattuale minima.

Se viene cessato l'abbonamento alla rete fissa o mobile esistente al momento della stipulazione del servizio (punto 3.1), anche i servizi per cui si è sottoscritto un abbonamento ai sensi delle presenti Condizioni dell'offerta terminano espressamente nello stesso momento in conformità al presente punto.

9.2 Promozioni

Una promozione può essere utilizzata dal cliente, per il servizio in oggetto, una sola volta. Al termine del periodo di promozione, il servizio diventa automaticamente a pagamento. La disdetta del servizio alla fine del periodo di promozione non autorizza il cliente a usufruire di un'altra promozione gratuita. Una nuova promozione gratuita non viene

concessa nemmeno nel caso in cui il cliente si abboni nuovamente al servizio in un momento successivo.

10 Modifiche

Swisscom si riserva il diritto di modificare in qualsiasi momento i prezzi, i servizi o le condizioni dell'offerta. Modifiche a svantaggio del cliente saranno comunicate da Swisscom in forma adeguata.

Qualora Swisscom aumenti i prezzi in maniera tale da incrementare il carico complessivo per il cliente o modifichi un servizio o le condizioni dell'offerta del cliente con un considerevole svantaggio per quest'ultimo, il cliente può disdire anticipatamente il servizio in questione entro la data di entrata in vigore della modifica senza subire conseguenze finanziarie. In caso contrario, il cliente accetta le modifiche. Gli adeguamenti dei prezzi in seguito a modifiche delle aliquote contributive (p.es. aumento dell'IVA) e l'aumento dei prezzi di fornitori terzi (in particolare con i servizi a valore aggiunto) non sono considerati come aumenti di prezzi e non autorizzano a una disdetta. Qualora Swisscom dovesse ridurre le tariffe, potrà contestualmente adattare di conseguenza gli sconti concessi prima della riduzione delle tariffe.