Condizioni generali del servizio

Rev	Del	Descrizione	Approvazione
0	21/11/2022	*Prima emissione*	*OK*

1. Premessa

Il presente documento si applica a tutte le distribuzioni del prodotto SaaS Shield. Tutti gli elementi non descritti nel documento o non presenti in offerta si intendono esclusi dal perimetro di erogazione.

2. Terminologia e definizioni

Fornitore: SI.net Servizi Informatici s.r.l., con sede legale in Milano, Corso Magenta 46, P.I./C.F. 02743730125, che fornisce il *servizio*.

Cliente: la persona giuridica o fisica che, per i propri scopi istituzionali/professionali, usufruisce del *servizio*.

Parti: il Fornitore e il Cliente

Contratto: l'accordo raggiunto tra le Parti a seguito dell'accettazione, da parte del Cliente, dell'offerta. Quest'ultima ha ad oggetto la fornitura del *servizio* secondo i termini in essa contenuti; insieme alle presenti Condizioni Generali e alla scheda prodotto, forma il Contratto.

Servizio: tutto quanto descritto dalle presenti Condizioni Generali, dall'offerta e dalla scheda prodotto.

Documento: il presente elaborato.

SaaS: acronimo di "software as a service", identifica la modalità di erogazione di un applicativo realizzato dal Fornitore. Il software distribuito non è installato localmente, ma viene messo a disposizione del Cliente tramite una connessione internet a fronte del pagamento di un canone per l'utilizzo del software stesso, non per il suo possesso.

3. Oggetto del servizio

Con il presente documento, il Fornitore si impegna a dotare il Cliente del servizio Cloud SaaS denominato "Shield". Tale servizio permetterà al Cliente di attivare un portale istituzionale in piena conformità rispetto al modello dei siti dei Comuni Italiani rilasciato da Designers Italia.

Poiché le tecnologie sono in costante evoluzione, quanto riportato nel presente documento descrive lo stato attuale del servizio. Al fine di assicurare servizi sempre aggiornati e best-in-class, il Fornitore si riserva di intervenire sullo stesso con apporti migliorativi.

Il servizio verrà erogato secondo le modalità descritte nel presente documento. Nessun'altra obbligazione al di fuori di quelle contenute nel presente documento verrà assunta dal Fornitore.

L'eventuale tolleranza di comportamenti, posti in essere da una o entrambe le parti, in violazione delle disposizioni contenute nel presente documento non costituisce rinuncia ai diritti derivanti dalle disposizioni violate né al diritto di esigere l'esatto adempimento delle obbligazioni e il rispetto dei termini e condizioni presenti nel documento stesso.

4. Caratteristiche del servizio

4.1. Descrizione del servizio

Il servizio Cloud SaaS Shield è la soluzione studiata dal Fornitore per dotare il Cliente di un sito istituzionale sviluppato su misura dei Comuni Italiani.

Il servizio è web oriented e sviluppato secondo le linee guida vigenti in materia di design, accessibilità e sicurezza.

Per maggiori dettagli circa architettura e funzionalità si rimanda alla scheda del prodotto.

4.2. Requisiti propedeutici all'attivazione del servizio

Connettività

Il Cliente si impegna a munirsi di una connettività adeguata, con avvertenza che, in difetto di tale connettività, qualora si riscontrassero dei rallentamenti durante l'utilizzo delle procedure software, nessuna responsabilità potrà essere attribuita al Fornitore.

Requisiti tecnico-amministrativi

Il Fornitore si riserva inoltre di non avviare le procedure di attivazione del servizio qualora il Cliente non abbia fornito tutte le informazioni propedeutiche all'onboarding e in particolare:

- Ordinativo o Determina
- Referente interno al Cliente
- Informazioni essenziali relative alla configurazione iniziale dell'applicativo, di cui si riportano a titolo esemplificativo:
  - Accesso al dominio (qualora non gestito dal Fornitore) e relativi record DNS attivi
  - Parametri ed eventuali autorizzazioni da fornitori di applicativi di terze parti per finalizzare integrazioni tramite API o web service;
  - Logo in formato vettoriale del Cliente
- Informativa privacy
- Nomina a responsabile esterno trattamento dati

4.3. Empty start-up

Il Fornitore, al momento dell'erogazione del software al Cliente, garantisce la completa assenza di dati e risorse all'interno dell'istanza risalenti a precedenti utilizzatori della stessa infrastruttura fisica o logica sottostante.

4.4. Cloud provider

Per l'erogazione del servizio il fornitore si avvale di cloud provider certificati e compliance con la normativa GDPR. Ulteriori dettagli sono illustrati al paragrafo Sicurezza del data center / cloud provider.

4.5. Sincronizzazione NTP

Il Fornitore utilizza all'interno della sua infrastruttura servizi NTP erogati da piattaforme certificate.

4.6. Indicazioni relative alla compatibilità delle tecnologie

La fruizione del servizio è consentita attraverso l'utilizzo di uno dei browser indicati di seguito:

- Firefox v.90+
- Chrome v.90+
- Safari v.13+
- Edge v.92+

4.7. Procedura di onboarding

La procedura di onboarding definisce l'iter di attivazione dell'applicativo dal momento in cui il Cliente formalizza l'ordine e il Fornitore lo riceve.

Il primo passo è quindi costituito dall'acquisto della soluzione che può avvenire tramite piattaforma di e-procurement o altro strumento di affidamento individuato dal Cliente.

Completate tutte le opportune procedure amministrative, il personale incaricato del Fornitore procederà alla richiesta delle informazioni propedeutiche di cui al paragrafo Requisiti propedeutici all'attivazione del servizio. Terminata la raccolta delle informazioni, entro i tempi indicati al paragrafo Tempi di attivazione, il Fornitore procederà con l'attivazione della piattaforma e con la configurazione dei parametri iniziali.

La fase di onboarding si intende conclusa con la trasmissione delle credenziali amministrative al referente tecnico del Cliente precedentemente individuato e condiviso con il Fornitore.

Tutto ciò che concerne l'attivazione di singole funzionalità supplementari, migrazione dei contenuti da sito precedente, configurazioni diverse da quelle iniziali, avverrà in seguito alla messa in produzione del portale base. Tutte le operazioni riguardanti tali attività potranno essere quindi concordate tra le Parti secondo i desiderata del Cliente e le disponibilità del Fornitore.

Il collaudo formale dell'applicativo sarà eseguito al termine della migrazione dei contenuti, in modo da effettuare una verifica puntuale su tutti gli elementi che concorrono alla corretta esecuzione dell'applicativo.

4.8. Tempi di attivazione

I tempi di attivazione del servizio decorrono dalla ricezione dell'ordine e sono specificati in offerta.

4.9. Modalità di accesso al servizio

Il front office è raggiungibile pubblicamente da internet attraverso connessione protetta HTTPS.

Il pannello di gestione del sito è invece accessibile tramite coppia di credenziali utente/password. Il rilascio delle credenziali, qualora non gestito in autonomia da parte del Cliente, avviene esclusivamente tramite sistema di ticketing verso soggetti specifici individuati dal Cliente.

5. Integrazioni con piattaforme e applicativi terzi comprese nel servizio

Shield è progettato per consentire l'integrazione a vari livelli con software di terze parti. Per il dettaglio delle integrazioni disponibili e comprese nel servizio si rimanda all'offerta.

6. Scalabilità del servizio

La scalabilità del servizio viene operata in base a due possibili condizioni: in conseguenza dell'attività di monitoraggio del servizio espletato secondo le procedure in essere ISO/IEC 27001 e/o in conseguenza di un ordine.

7. Servizio di assistenza standard

Il servizio comprende l'accesso ad un canale dedicato e regolamentato da un sistema di ticketing all'avanguardia, sottoposto alle nostre procedure certificate ISO/IEC 27001 e relative estensioni 27017 e 27018.

Il servizio di assistenza è inoltre accessibile tramite e-mail o telefono verso il centralino del Fornitore secondo il seguente piano orario: lunedì – venerdì, dalle 09:00 alle 13:00 e dalle 14:00 alle 18:00.

Si intendono comprese nel servizio di assistenza tutte quelle attività di supporto al Cliente che garantiscono la corretta fruizione del servizio, di cui a titolo esemplificativo si citano:

- richiesta di creazione nuovi utenti
- richiesta di supporto tecnico rispetto all'utilizzo dell'applicativo
- segnalazioni di errori/malfunzionamenti

In merito alla creazione di nuove utenze, si dovrà concordare insieme al Cliente il referente o i referenti autorizzati ad effettuare questo tipo di richiesta.

Il sistema di ticketing funge da canale principale anche per attivare procedure di change che possono non essere comprese nel contratto e comportare quotazioni specifiche, quali ad esempio:

- richiesta di attivazione di nuove funzionalità
- richiesta di nuove risorse/evoluzione risorse in uso
- richiesta di rapporti statistici
- richiesta di report relativi a utilizzo risorse
- richiesta di report relativi ad attività di VA/PT

8. Servizio di manutenzione standard

La gestione, il monitoraggio e la manutenzione della piattaforma di erogazione in tutte le sue componenti sono in carico al Fornitore. Si intendono comprese nel servizio tutte quelle attività atte a garantire la corretta erogazione del servizio a livello applicativo e infrastrutturale secondo le best practise e gli standard ISO del Fornitore.

Non sono compresi nel servizio di manutenzione standard:

- tutte le attività che prevedono un'estensione delle risorse disponibili indicate in offerta
- estensioni delle policy di backup applicate
- personalizzazioni o customizzazioni dell'applicativo

9. Reportistica

Il Cliente può richiedere in ogni momento, a mezzo ticket, lo stato di funzionamento ed utilizzo delle risorse da parte dell'applicativo secondo le metriche legate al piano di erogazione SaaS.

Eventuali reportistiche specifiche, che prevedono l'impego di metriche differenti da quelle esistenti, potranno essere sviluppate al di fuori dell'offerta standard e quotate in relazione alle specifiche esigenze del Cliente.

10. Backup

La policy di backup applicata dal Fornitore è strutturata secondo il piano seguente:

- Portale e DB:
  - Un punto di ripristino ogni giorno con retention di 28 giorni
- Archivio documentale:
  - Un punto di ripristino ogni mese con retention di 40 giorni

Inoltre, viene effettuato un export del DB con replica su diverso Cloud provider certificato secondo il piano seguente:

- Un punto di ripristino ogni giorno con retention di 28 giorni

Si precisa che il cloud provider individuato adotta opportune politiche e misure di replica e disaster recovery al fine di garantire in ogni momento disponibilità, sicurezza e monitoraggio del dato.

Eventuali policy di backup estese rispetto a quanto indicato nel presente documento o in offerta costituiscono una procedura di change del servizio che può essere richiesta tramite sistema di ticketing previa quotazione economica.

11. SLA

Il livello di servizio del software è misurabile sulla base dei seguenti parametri di funzionalità operativa:

- Disponibilità degli applicativi: Uptime del 90% su base annuale.
- Presa in carico dei ticket: 8 ore lavorative
- Risoluzione ticket bloccanti: NBD

12. Durata del servizio

La durata del servizio è regolata da quanto definito in offerta e formalizzato dal Cliente tramite l'acquisto. Il Fornitore indica i riferimenti di inizio e termine attività in offerta.

12.1. End of service (reversibilità del servizio)

In caso di mancato rinnovo del servizio, il Cliente dovrà richiedere i dati al Fornitore tramite Pec con un anticipo di almeno trenta giorni rispetto alla scadenza del contratto.
Qualora il termine sopra indicato non venga rispettato, il Fornitore si riserva di applicare i relativi costi di gestione per il periodo necessario alle attività di end of service.
Decorsi sei mesi dalla scadenza del contratto il Fornitore procederà alla cancellazione di tutti i dati di proprietà del Cliente presenti sulla propria infrastruttura.
In merito all'esportazione della parte documentale, il Cliente può richiedere tramite ticket di effettuare un'esportazione massiva dei contenuti conservati. Tale esportazione, opportunamente crittografata, verrà inviata al Cliente tramite metodo concordato.

13. Elementi non compresi nel servizio (offerta standard)

13.1. Storage

Il Servizio offerto include una specifica quantità di spazio pre-allocato per il Cliente: il limite e la relativa soglia di allerta sono definiti in offerta. Oltre la soglia indicata, il Fornitore procederà a notificarne al Cliente il superamento nella persona del referente tecnico indicato nella documentazione contrattuale.
Eventuali consumi sopra soglia non si intendono compresi nel servizio standard e dovranno essere opportunamente quotati.
Si precisa che il superamento del limite indicato potrebbe comportare il blocco del servizio.

13.2. Ripristino

Il Fornitore offre la possibilità al Cliente di sfruttare il backup infrastrutturale compreso nel servizio per il ripristino di risorse e componenti relativi alla propria istanza in uno dei punti di ripristino disponibili. Si evidenzia che le attività di ripristino infrastrutturale devono essere acquistate separatamente.

13.3. Integrazioni software terze parti

Grazie alla grande flessibilità del prodotto, Shield può essere esteso tramite componentistica applicativa sviluppata su misura per l'integrazione verso sistemi terzi messi a disposizione dal Cliente. Si evidenzia che, in assenza di specifiche voci riportate in offerta, le attività non sono comprese nell'offerta standard.

Per avviare le attività di sviluppo custom, il Fornitore si riserva di valutare i seguenti requisiti:

- analisi preliminare
- disponibilità di documentazione relativa a software oggetto dell'integrazione verso Shield
- disponibilità di un ambiente di test messo a disposizione dal Cliente
- riferimento tecnico relativo al software oggetto dell'integrazione verso Shield

13.4. Personalizzazioni

Se non espressamente indicato in offerta, tutte le attività che riguardano personalizzazioni dell'applicativo e la loro relativa manutenzione sono da intendersi escluse dall'offerta standard e dovranno essere quotate separatamente previa analisi di fattibilità ed esecuzione delle specifiche esigenze del Cliente.

13.5. Backup aggiuntivi

Oltre a quanto descritto al paragrafo Backup, il Cliente ha la facoltà di richiedere in qualsiasi momento l'attivazione di policy estese rispetto a quelle definite dalle nostre misure standard. Eventuali modalità, specifiche e attività saranno definite a seguito di analisi preliminare delle esigenze del Cliente.

14. Politica di uso accettabile del servizio

Il Fornitore adotta nell'ambito delle proprie procedure certificate ISO/IEC 27001 una politica sull'uso accettabile rispetto ai servizi erogati.

L'utente (il Cliente) non può utilizzare, facilitare o consentire ad altri di utilizzare, i Servizi erogati dal Fornitore:

- per qualsiasi attività illegale o fraudolenta;
- violare i diritti degli altri;
- per minacciare, incitare, promuovere o incoraggiare attivamente la violenza, il terrorismo o altri gravi danni;
- per qualsiasi contenuto o attività che promuova lo sfruttamento o l'abuso sessuale di minori;
- violare la sicurezza, l'integrità o la disponibilità di qualsiasi utente, rete, computer o sistema di comunicazione, applicazione software o rete o dispositivo informatico;

- per distribuire, pubblicare, inviare o facilitare l'invio di e-mail di massa non richieste o altri messaggi, promozioni, pubblicità o sollecitazioni (o "spam").

Per ulteriori dettagli si rimanda al documento specifico.

15. Responsabilità condivisa

La sicurezza e la conformità del servizio sono definite da un modello di responsabilità condivisa tra il Fornitore e il Cliente. Questo modello può aiutare e supportare il Cliente nel comprendere il perimetro di azione e intervento del Fornitore e quanto, al contrario, resta a carico del Cliente.

Nel caso dei servizi SaaS, Il Fornitore è responsabile di tutto lo strato applicativo secondo la ratio del garantire la corretta erogazione del servizio stesso. Accanto al "nudo" servizio, il Fornitore completa la propria offerta garantendo al cliente una serie di opzioni aggiuntive che, tuttavia, restano circoscritte a precisi ambiti di applicazione.

Resta quindi a carico del Cliente tutto ciò che esula da questo strato.

Per ulteriori dettagli relativi al modello si rimanda al documento specifico.

16. Logging

Il Fornitore mantiene log a tre livelli per l'erogazione del servizio Shield:

1. Un log a livello applicativo per la visualizzazione di tracciamenti ad alto livello;
2. Un log a livello di piattaforma, che permette di tenere traccia delle transazioni API e dello scambio di comunicazione tra i componenti;
3. Un log a livello di infrastruttura che permette di listare eventuali attività sull'architettura portante del software.

Il cliente ha accesso indipendente al primo tracciato e può richiedere parti del secondo via ticket specificando una data di interesse.

Il terzo log è interno al Fornitore e viene utilizzato dallo staff per garantire la conformità a quanto descritto in questo documento.

L'accesso alle informazioni di log è esclusivamente concesso per scopi di debug, ottimizzazione delle performance e verifiche di funzionamento dell'applicativo.

17. Trattamento dati

17.1. Posizionamento geografico dei dati

Il Fornitore ospita i dati all'interno di data center ad alta sicurezza ed affidabilità ospitati esclusivamente su territorio europeo. Il Cliente può comunque richiedere in ogni momento informazioni puntuali sul posizionamento dei suoi dati e delle sue risorse cloud.

17.2. Titolarità nel trattamento dei dati

Il Fornitore agisce da Titolare del trattamento dei dati quando raccoglie dati personali e determina le finalità e le modalità per il loro trattamento (ad esempio, quando il Fornitore memorizza le informazioni necessarie per la registrazione e l'amministrazione di un account, l'accesso ai servizi o le informazioni di contatto per fornire assistenza tramite il supporto clienti). In tutti gli altri casi il titolare dei dati è il Cliente e il Fornitore si configura come responsabile esterno.

17.3. Trattamenti fuori ambito

Il Fornitore, all'interno dell'accordo regolato da questo documento, in nessun caso tratta i dati dei clienti al di fuori dell'ambito di erogazione del servizio e della messa in sicurezza delle informazioni.

Inoltre, il Fornitore non effettua diffusioni di dati personali al di fuori della collaborazione con i sub-fornitori che agiscono come data processor e ospitano fisicamente dati e risorse.

17.4. Accesso da parte delle autorità e trasferimenti dati a eventuali processor

Il Fornitore notificherà, ai riferimenti tecnici ed amministrativi del Cliente, riportati nella documentazione contrattuale, qualsiasi richiesta legalmente vincolante di divulgazione di dati personali da parte di un'autorità giudiziaria, a meno che tale divulgazione non sia altrimenti vietata.

Il Fornitore opera i servizi cloud qui descritti utilizzando l'infrastruttura fisica dei sub-fornitori che agiscono come data processor in conformità alla certificazione ISO/IEC 27001.

18. Sicurezza del servizio

Il Fornitore è possesso della certificazione secondo lo standard ISO/IEC 27001 estesa con i controlli degli standard ISO/IEC 27017 e ISO/IEC 27018

Il Fornitore si impegna inoltre, ai sensi dall'art. 32 del GDPR, ad adottare le opportune misure fisiche, logiche e organizzative atte a garantire la sicurezza del proprio servizio.

18.1. Sicurezza del data center / cloud provider

I data center sui quali sono ospitati i servizi erogati dal Fornitore garantiscono il massimo livello di tecnologia, sicurezza e affidabilità presente sul mercato. In particolare, il Cloud Provider scelto dal Fornitore è in possesso di tutte le certificazioni di sicurezza atte a garantire i migliori livelli di disponibilità e ridondanza del dato.

Il Cloud Provider è in possesso, inoltre, di opportune politiche di disaster recovery, monitoring degli asset e degli accessi, controllo del clima e della temperatura dei locali, gestione del rischio e manutenzione e sorveglianza delle risorse e delle strutture.

I dettagli circa le misure di sicurezza adottate dal Cloud Provider individuato dal Fornitore possono essere richiestI tramite sistema di ticketing.

18.2. Procedura di incident

La procedura di incident è regolamentata dal sistema ISO/IEC 27001 e prevede due perimetri di intervento.

In caso di rilevazione di un incident da parte del Cliente, la comunicazione dello stesso può avvenire tramite il sistema di ticketing.

Qualora sia il Fornitore a rilevare l'incident attraverso i propri sistemi di monitoraggio, i tecnici incaricati procederanno con le opportune verifiche sulla superficie di impatto dell'evento, il quale verrà comunicato al riferimento tecnico del Cliente in forma di avviso generico e/o di manutenzione straordinaria.

Il Cliente può richiedere informazioni circa la procedura di risoluzione ed eventuali rimedi temporanei tramite ticket.

18.3. Evidenze di conformità

In qualunque momento il Cliente, tramite il portale di ticketing, può richiedere al Fornitore evidenze di conformità ISO/IEC 27001 cui il Fornitore è tenuto a dar riscontro con effettiva certificazione o prove puntuali di conformità nel rispetto della propria politica di sicurezza.

18.4. Rapporti di VA/PT

È facoltà del Cliente richiedere tramite ticket rapporti generici riguardanti gli esiti delle attività di VA/PT effettuati periodicamente dal Fornitore.

Qualora il Cliente voglia effettuare in autonomia o tramite soggetti terzi attività di VA/PT su servizi in produzione o ambiente dedicato, è necessario comunicare preventivamente al Fornitore l'esigenza e concordare date e modalità di esecuzione, al fine di non pregiudicare il corretto funzionamento del Servizio. Il Fornitore non risponde di eventuali blocchi, malfunzionamenti o disservizi applicativi qualora questa disposizione venga disattesa dal Cliente.

Si ricorda, inoltre, che, in caso di eventuali disservizi infrastrutturali che contravvengono alle policy del Cloud Provider causati da attività non concordate con il Fornitore, potranno essere intraprese azioni legali da parte del Fornitore e/o delle parti coinvolte.

19. Impegno sulla sostenibilità ambientale

Il servizio cloud SaaS Shield rappresenta un valido strumento ai fini della transizione verde. I servizi digitali permettono, innanzitutto, di ridurre significativamente l'impiego di nuove risorse materiali (es. carta). Dematerializzare significa, inoltre, minimizzare gli spostamenti: i destinatari dei servizi non dovranno più recarsi presso la sede del Cliente, se non quando strettamente necessario.

Il Fornitore si impegna inoltre ad avvalersi di cloud provider sensibili rispetto al tema della sostenibilità e che adottano opportune politiche rispetto all'impatto ambientale.