multiSign cloud

CONDIZIONI GENERALI DI CONTRATTO

ver. 3 - 20/05/2023

Riepilogo

1 DEFINIZIONI _ 5

2 STRUTTURA E OGGETTO CONTRATTUALE 6

3 DURATA DEL CONTRATTO, RINNOVO E RISOLUZIONE 6

4 TARIFFE E MODALITÀ DI PAGAMENTO 6

5 MANCATO PAGAMENTO 6

6 OBBLIGHI, GARANZIE E LIMITAZIONI DI RESPONSABILITÀ DEL FORNITORE 6

6.1 GARANZIE DEL FORNITORE 6
6.2 SLA 6
6.3 LIMITAZIONI DELLE GARANZIE 6
6.4 AUDIT DI SECONDA PARTE 7
6.5 GARANZIA DI RIMBORSO PER MANCATA ATTIVAZIONE 7
6.6 LIMITAZIONI DI RESPONSABILITÀ 7
6.7 INTEROPERABILITÀ CON APPLICAZIONI DI TERZE PARTI 7
6.8 MODIFICHE AL SERVIZIO 7
6.9 CONSERVAZIONE DEI DATI 7
6.10 POSIZIONE DEI DATACENTER 7
6.11 RISARCIMENTO 7
6.12 ESCLUSIONI 8

7 SUBAPPALTATORI 8

7.1 REQUISITI DI SICUREZZA 8
7.2 PROTEZIONE DATI 8
7.3 NOTIFICA CAMBIO SUBAPPALTATORE 8

8 DIRITTI E OBBLIGHI DEL CLIENTE 8

8.1 INTEROPERABILITÀ DI DATI, APPLICAZIONI DI TERZE PARTI E FORNITORI 8
8.2 GARANZIE E RESPONSABILITÀ DEL CLIENTE 9
8.3 RISARCIMENTO 9
8.4 INFORMAZIONI DI SICUREZZA 9
8.5 OBBLIGHI DEL CLIENTE 10

9 SUPPORTO E MANUTENZIONE 10

9.1 MONITORAGGIO DELLE PRESTAZIONI 10
9.2 MANUTENZIONE DI EMERGENZA. 10
9.3 AGGIORNAMENTI. 10
9.4 SERVIZI DI SUPPORTO 10
9.5 SERVIZI PROFESSIONALI 10

10 SOSPENSIONE DEL SERVIZIO 11

11 CLAUSOLA RISOLUTIVA ESPRESSA – RISOLUZIONE PER INADEMPIENZA – CONDIZIONI RISOLUTIVE 11

12 RITIRO 11

13 MODIFICHE DEL CONTRATTO E/O DELLE POLITICHE DEL FORNITORE 11

14 COPYRIGHT E LICENZE 11

15 INFORMAZIONI DI SICUREZZA 11

15.1 SOSPENSIONE DEL SERVIZIO 11
15.2 SEGREGAZIONE DI RETE 11
15.3 RAPPORTO SULL'INCIDENTE DI SICUREZZA 11
15.4 SUBAPPALTATORI 11
15.5 RILEVAMENTO DELLE VULNERABILITÀ 11

16 DENUNCE, CONTESTAZIONI 12

17 TRATTAMENTO DEI DATI PERSONALI 12

17.1 GDPR 12
17.2 TITOLARE DEL TRATTAMENTO E RESPONSABILE DEL TRATTAMENTO 12
17.3 LIMITI AL TRATTAMENTO DEI DATI 12
17.4 DATI PERSONALI 12
17.5 PROTEZIONE DEI DATI DI TERZE PARTI 12
17.6 OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO 12
17.7 RICHIESTE DI COMUNICAZIONE DEI DATI 12
17.8 RESPONSABILE DELLA PROTEZIONE DEI DATI 12
17.9 VIOLAZIONE DEI DATI 13

18 LEGGE APPLICABILE E FORO COMPETENTE 13

19 NOMINA A RESPONSABILE DEL TRATTAMENTO 13

20 MISURE TECNICHE 14

20.1 FIREWALL 14
20.2 PROTEZIONE DAI MALWARE 14
20.3 CREDENZIALI DI AUTENTICAZIONE 14
20.4 PAROLA D'ORDINE 14
20.5 REGISTRAZIONE 14
20.6 RIPRISTINO DEL BACKUP 14
20.7 VALUTAZIONE DELLA VULNERABILITÀ E TEST DI PENETRAZIONE 14
20.8 AMMINISTRATORI DI SISTEMA 14
20.9 BANCA DATI 14
20.10 SICUREZZA DELLE COMUNICAZIONI 14
20.11 CRITTOGRAFIA 15
20.12 HARDENING 15
20.13 CANCELLAZIONE SICURA DI DATI E FILE TEMPORANEI 15
20.14 OROLOGIO DI SINCRONIZZAZIONE 15
20.15 SVILUPPO SICURO 15

21 MISURE ORGANIZZATIVE 16

21.1 POLITICHE E REGOLAMENTI 16
21.2 ACCESSO LOGICO 16

21.3 SUPPORTO ALLA GESTIONE DELLE OPERAZIONI 16
21.4 GESTIONE DEGLI INCIDENTI 16
21.5 GESTIONE DELLE VIOLAZIONI DEI DATI 16
21.6 FORMAZIONE 16
21.7 GESTIONE DEL CAMBIAMENTO 16
21.8 AUDIT INTERNO 16
21.9 CERTIFICAZIONI 16
21.10 LIMITAZIONI ALL'UTILIZZO DEL SERVIZIO 17
21.11 VIOLAZIONI 17
21.12 PROVE DI VULNERABILITÀ 17

1 DEFINIZIONI _

TERMINE	DEFINIZIONE
Disponibilità	La garanzia della disponibilità minima del servizio sottoscritto, misurata in percentuale sulla base dei mesi solari per la durata del servizio
Contratto	L'insieme che comprende le Condizioni Generali e tutti i Contratti o Ordini o Sottoscrizioni
Cliente	La società, o altra entità, che sottoscrive un Contratto soggetto alle Condizioni Generali
Documentazione	Le istruzioni e le spiegazioni online, i manuali e altri documenti scritti o registrati, compresi i video, e qualsiasi manuale fornito dal Fornitore relativo all'utilizzo del Servizio
Eventi di forza maggiore	Tutto ciò che non è ragionevolmente prevedibile e controllabile da una delle parti contraenti, come terremoti, alluvioni o altri interventi naturali; atti di guerra, ostilità e sabotaggio; guasto della rete elettrica, delle telecomunicazioni o di Internet, non causato direttamente da uno degli appaltatori, o normativo e vincolante
Diritti di proprietà intellettuale	Brevetti, diritti d'autore, modelli, marchi, design registrati, diritti morali, diritti di design (registrati e non), know-how, database, nomi e marchi, i diritti su informazioni e dati proprietari e ogni altro diritto proprietario (incluse le relative richieste di registrazione, e il diritto di richiedere la registrazione o la tutela dei diritti sopra elencati), esistenti o applicabili in qualsiasi parte del mondo
Manutenzione	Manutenzione, aggiornamenti, installazione di nuove versioni e riparazioni di hardware e software
Servizio	Il servizio cloud di firma digitale fornito al Cliente: https://www.itagile.it/multisign-cloud/?lang=it Il servizio è nell'Unione Europea e fornito a livello globale
SLA	Accordo sul livello di servizio
Fornitore	itAgile SRL, con sede legale in Viale America 111, Roma, PEC: itagile@pec.it
Applicazione di terze parti	Un'applicazione Internet online o un prodotto software offline, fornito o concesso in licenza da terzi e che interagisce con il Servizio (ad esempio, browser)
Aggiornamento	Qualsiasi modifica, correzione di errore o miglioramento apportato al Servizio
Utenti	Dipendenti, dirigenti, consulenti, soci, uffici, subappaltatori del Cliente ed in genere coloro che agiscono per conto del Cliente o in relazione con il Cliente, che ricevono un codice utente e/o una password (le credenziali) per accedere al Servizio

2 STRUTTURA E OGGETTO CONTRATTUALE

Il presente contratto regola il rapporto tra Fornitore e Cliente durante il periodo di erogazione del Servizio. Il contratto viene sottoscritto implicitamente dal Cliente al momento dell'attivazione del Servizio. La cessione a terzi, in tutto o in parte, definita come "rivendita" del Servizio, è consentita fatte salve le responsabilità e le limitazioni qui previste. Eventuali servizi accessori richiesti dal Cliente anche successivamente alla conclusione del presente Contratto sono soggetti alle medesime condizioni e sono considerati parte integrante del servizio. Qualora nell'ordine del Cliente sia impostata una diversa condizione e l'ordine venga accettato dal Fornitore, la diversa condizione è valida solo se riferita al presente contratto, definendo esplicitamente la versione contrattuale ed il paragrafo interessato. Lo schema contrattuale è il noleggio delle cose, cioè la licenza d'uso. Il cliente non acquisirà mai la proprietà dei servizi forniti.

3 DURATA DEL CONTRATTO, RINNOVO E RISOLUZIONE

La durata del contratto è definita nell'offerta commerciale che il Cliente sottoscrive inviando l'ordine al Fornitore o attivando il Servizio online. I servizi sottoscritti forniti con clausola di rinnovo automatico nell'offerta accettata, si rinnovano automaticamente alla scadenza, per lo stesso periodo e alle stesse condizioni. In caso di rinnovo automatico, il Cliente può disdire il servizio - inviando una comunicazione scritta al Fornitore o aprendo un ticket - entro cinque giorni prima della scadenza.

4 TARIFFE E MODALITÀ DI PAGAMENTO

I corrispettivi sono definiti nell'offerta commerciale sottoscritta dal Cliente online o con l'invio dell'ordine al Fornitore. L'offerta commerciale definisce le modalità di pagamento del servizio.

5 MANCATO PAGAMENTO

Il Fornitore - nel caso in cui il Cliente non provveda al pagamento del Servizio entro i termini definiti nell'offerta sottoscritta - può sospendere o annullare il Servizio. In caso di sospensione o cancellazione, il Fornitore si riserva il diritto di chiedere al Cliente un risarcimento per il ripristino del Servizio.

6 OBBLIGHI, GARANZIE E LIMITAZIONI DI RESPONSABILITÀ DEL FORNITORE

6.1 Garanzie del fornitore

Il Fornitore garantisce per il Servizio: (i) di avere il diritto di concedere in licenza il software che costituisce il Servizio; (ii) che tale software funzionerà come descritto nella Documentazione; (iii) di avere il diritto di concedere la licenza per utilizzare l'Applicazione di Terze Parti; (iv) che il Servizio sarà prestato con adeguata competenza, diligenza e professionalità, in linea con le attuali best practice aziendali del settore; e (v) che il Servizio sarà fornito in conformità con lo SLA definito nel presente Contratto.

6.2 SLA

Il livello di servizio garantito è del 99,95% su base annua. In caso di superamento di tale limite, il Fornitore riconoscerà al Cliente un credito pari all'1% del costo del servizio annuo, per ogni 30 minuti di superamento della soglia di disponibilità garantita fino ad un massimo di 300 minuti.

6.3 Limitazioni delle garanzie

Le garanzie di cui all'articolo 6.1 non coprono eventuali carenze o danni dovuti a: (i) interazione con Applicazioni di terzi e/o con software, servizi o contenuti di terzi; (ii) qualsiasi connettività fornita da terze parti; (iii) qualsiasi modifica al Servizio non effettuata dal Fornitore o (iv) qualsiasi operazione diversa da quanto indicato nella Documentazione che sia causata da un utilizzo del Servizio non conforme alle Condizioni d'Uso del Servizio.

Salvo quanto espressamente stabilito nel presente Contratto, sono escluse tutte le garanzie e condizioni, espresse o implicite, previste dalla legge, dai regolamenti o da altra fonte nella misura massima consentita dalla legge o, comunque, per il restante importo del contratto. Non viene prestata alcuna garanzia in merito ai risultati che il Cliente può ottenere dal Servizio né che il Servizio funzionerà senza interruzioni e senza errori.

6.4 Audit di seconda parte

Il Cliente può richiedere audit di seconda parte. Ove la richiesta non possa essere soddisfatta, il Fornitore mette a disposizione la visione della documentazione e dei relativi certificati ottenuti in conformità alle norme UNI CEI ISO/IEC 27001:2017 – ISO/IEC 27017:2015 – ISO/IEC 27018:2019.

6.5 Garanzia di rimborso per mancata attivazione

Se il servizio viene pagato prima dell'attivazione e il servizio non può essere attivato per motivi tecnici, il fornitore applica la politica di "soddisfatti o rimborsati".

6.6 Limitazioni di responsabilità

Il Fornitore non sarà in ogni caso responsabile per errori, perdite o danneggiamenti dei dati del cliente, anche se i dati non sono gestiti attraverso il Servizio stesso, o quanto sopra è conseguenza di difetti nei processi di caricamento dei dati, anche se l'estrazione di i dati dal Database del Cliente e/o il caricamento dei dati nel Database del Cliente sono stati effettuati utilizzando strumenti di interoperabilità, come interfacce di programmazione dell'applicazione (API) o altri componenti software di servizio o supporto che possono essere forniti dal Fornitore.

6.7 Interoperabilità con applicazioni di terze parti

Il Fornitore può includere nel Servizio funzionalità basate sull'interoperabilità con Applicazioni di terzi (ad esempio, applicazioni DocuSign o certificati TrustPro). Il Fornitore non offre alcuna garanzia circa la disponibilità nel tempo di tali applicazioni se tali applicazioni non sono fornite direttamente dal Fornitore. Il Cliente prende atto che, qualora un fornitore cessi di rendere disponibile un'Applicazione di Terze Parti per l'interoperabilità con il Servizio, il Fornitore potrà, a sua discrezione, rimuovere la corrispondente funzionalità dal Servizio senza alcuna sostituzione con un'altra Applicazione di Terze Parti.

6.8 Modifiche al servizio

Il Fornitore potrà apportare modifiche al Servizio modificando quanto descritto nella Documentazione. Se necessario, le modifiche vengono comunicate al Cliente tramite e-mail. Tali modifiche possono includere, ad esempio: (i) modifiche alle configurazioni minime delle apparecchiature (come i computer) necessarie per utilizzare il Servizio; (ii) modifiche alle regole di utilizzo, regole di sicurezza e riservatezza, o nuove regole per garantire la sicurezza e l'integrità del Servizio; (iii) modifiche alle Condizioni Generali relative ad Applicazioni di Terzi e contenuti messi a disposizione dal Fornitore; (iv) limiti sulla quantità di spazio di memoria che può essere utilizzato per i dati del cliente (inclusi i Documenti Aggiuntivi del cliente) e restrizioni simili volte ad evitare carichi irragionevoli sul Servizio; e/o (v) regole per garantire che i database e le applicazioni facenti parte del Servizio possano essere utilizzati nel modo più efficace possibile e nei limiti delle capacità disponibili.

6.9 Conservazione dei dati

Il Fornitore garantisce la conservazione dei dati del Cliente per tutto il periodo di validità del contratto secondo le migliori pratiche di sicurezza e nel rispetto del regolamento europeo per la protezione dei dati personali 2016/679. Il Fornitore garantisce la cancellazione sicura dei dati del Cliente, ad eccezione dei dati relativi al certificato di firma digitale e dei dati relativi agli adempimenti fiscali del Fornitore, esclusivamente su esplicita richiesta del Cliente: (i) al termine del periodo di validità del Contratto; (ii) a seguito della risoluzione del contratto. La cancellazione sicura dei dati del cliente avverrà secondo le procedure del Fornitore.

6.10 Posizione dei datacenter

Il Fornitore garantisce che i datacenter del Servizio si trovano nell'Unione Europea, il Servizio utilizza soluzioni di co-location nei seguenti datacenter:

- Aruba Terme – Arezzo
- TrustPro Ltd - Dublino
- itAgile - Roma

6.11 Risarcimento

Qualora il Servizio, o parte di esso, divenga oggetto di azione legale o denuncia di violazione, il Fornitore potrà a proprie spese ed a propria discrezione: (i) concedere al Cliente la facoltà di continuare ad utilizzare il Servizio o parte del Servizio in questione; (ii) sostituire il Servizio o parte del Servizio con un altro servizio o software che

non consenta la stessa violazione; (iii) modificare il Servizio o parte del Servizio al fine di eliminare la causa della violazione; ovvero, qualora nessuna delle opzioni fin qui elencate sia possibile, (iv) risolvere il contratto del Cliente per quell'elemento del Servizio che contiene la controparte, dandone preavviso scritto di 30 giorni, e restituire al Cliente l'eventuale corrispettivo prepagato a tale elemento per la parte del Periodo Contrattuale successivo alla data di recesso.

6.12 Esclusioni

Il Fornitore non avrà alcuna responsabilità né obbligo di intervento, in caso di errori, problemi o malfunzionamenti, né in caso di mancata disponibilità del Servizio, quando questi derivino da una delle seguenti cause: (i) violazioni degli obblighi del Cliente derivanti dal presente Contratto; (ii) errori od omissioni degli Internet Service Provider; (iii) utilizzo di Applicazioni di Terze Parti, o funzionalità di "Single Sign-On" che il Cliente o un Utente ha installato e/o abilitato per accedere al Servizio o per interagire con esso, inclusi i casi di diffusione, modifica o cancellazione dei Dati del Cliente ; (iv) la sottovalutazione di attacchi informatici o incidenti simili; (v) eventuali problemi DNS che non sono sotto il controllo del Fornitore, ad esempio errori nella rete del Cliente o nella rete di un fornitore di servizi Internet; (vi) eventuali problemi o errori che si verificano mentre il Fornitore è in attesa che il Cliente fornisca informazioni utili per correggere un errore o ripristinare i servizi; (vii) inconvenienti causati dalle attività gestionali od operative del Cliente relative al Servizio; (viii) Forza Maggiore.

7 Subappaltatori

7.1 Requisiti di sicurezza

Il Fornitore può avvalersi di subappaltatori nella fornitura del Servizio. Il Fornitore, per garantire che i subappaltatori rispettino i requisiti per la sicurezza delle informazioni del Fornitore, seleziona subappaltatori con certificazioni equivalenti alle certificazioni del Fornitore e si riserva la possibilità di effettuare audit di seconda parte del Subappaltatore

7.2 Protezione dati

Qualora il Fornitore trasferisca dati personali al Subappaltatore, tali dati saranno riportati all'interno della nomina a titolare del trattamento.

7.3 Notifica cambio subappaltatore

Il Fornitore, prima della modifica di un subappaltatore, comunica al Cliente tale modifica, prima che questa venga attuata.

8 DIRITTI E OBBLIGHI DEL CLIENTE

8.1 Interoperabilità di dati, applicazioni di terze parti e fornitori

8.1.1 - Se il Cliente utilizza prodotti o servizi di terze parti, incluse, a titolo esemplificativo ma non esaustivo, altre applicazioni non fornite dal Fornitore e/o localizzazione, configurazione, servizi di consulenza forniti da terze parti e/o se il Cliente scambia dati relativi al servizio con un fornitore di terze parti, incluso il caso di utilizzo di API (Application Programming Interface) fornite dal Fornitore per l'accesso ai Dati del Cliente, qualsiasi accordo relativo a queste operazioni è esclusivamente tra il Cliente e il fornitore di terze parti del prodotto o del servizio. Il Fornitore non fornisce alcuna garanzia o assistenza su prodotti o servizi di terzi, anche se questi sono stati consigliati dal Fornitore.

8.1.2 - Se il Cliente installa o abilita Applicazioni o servizi di terze parti (ad esempio, "servizi web") che possono essere utilizzati con il Servizio, il Cliente riconosce che il Fornitore può consentire ai fornitori di tali Applicazioni o Servizi di terze parti di accedere ai dati dei clienti per consentire l'interoperabilità con il Servizio. Il Fornitore non si assume alcuna responsabilità in caso di divulgazione, modifica o perdita dei Dati del Cliente causata da Applicazioni di Terzi o fornitori di servizi.

8.1.3 - Nei casi indicati ai precedenti punti del presente articolo, il Cliente dovrà richiedere esplicita autorizzazione al Fornitore aprendo un ticket utilizzando il servizio di assistenza all'indirizzo https://support.itagile.it
.

8.2 Garanzie e responsabilità del cliente

8.2.1 – Il Cliente garantisce di disporre di tutti i diritti d'uso, diritto d'autore e diritti connessi necessari per adempiere alle proprie obbligazioni derivanti dal presente Contratto.

8.2.2 - Il Cliente accetta ed è consapevole che le garanzie di cui all'articolo 8.2.1 non coprono eventuali carenze o danni dovuti a: (i) interazione con Applicazioni di Terzi e/o con software, servizi o contenuti non del Fornitore; (ii) qualsiasi connettività fornita da terze parti; (iii) qualsiasi modifica al Servizio non effettuata dal Fornitore; o (iv) qualsiasi operazione diversa da quanto dichiarato nella Documentazione che sia causata dall'utilizzo del Servizio in modo non conforme ai Termini del presente Contratto.

8.2.3 - Il Cliente accetta che, salvo quanto espressamente stabilito nel presente Contratto, tutte le garanzie e condizioni, esplicite o implicite, previste dalla legge, dai regolamenti o da altra fonte sono escluse nella misura massima consentita dalla legge. Non viene prestata alcuna garanzia circa i risultati che il Cliente può ottenere utilizzando il Servizio né che il Servizio funzionerà senza interruzioni e senza errori.

8.2.4 - Il Cliente sarà responsabile di ogni violazione del presente Contratto dovuta ad azioni, omissioni o negligenze degli Utenti o di altri soggetti che accedono al Servizio con il codice di accesso del Cliente, come se tali azioni, omissioni o negligenze fossero state commesse dal Cliente direttamente.

8.2.5 - Il Cliente garantisce di disporre di tutti i diritti d'uso, di rispettare il diritto d'autore e gli eventuali diritti connessi, necessari per l'utilizzo di qualsiasi tipo di software utilizzato in ambiente cloud.

8.2.6 - Il Cliente garantisce che le licenze fornite dal Fornitore siano utilizzate entro i limiti previsti dal Fornitore.

8.3 Risarcimento

Il Cliente risarcirà il Fornitore e i suoi dipendenti, subappaltatori e coloro che agiscono per suo conto tutti i costi, le perdite, le spese dovute a terzi, incluse le ragionevoli spese legali, derivanti da controversie relative o risultanti direttamente o indirettamente da: (i) violazioni da parte del Cliente o Utente di qualsiasi Diritto di Proprietà Intellettuale in relazione all'utilizzo del Servizio effettuato al di fuori delle disposizioni del presente Contratto; (ii) il trattamento da parte del Fornitore dei dati, inclusi i dati personali, del Cliente, di altri elementi del Cliente o forniti dal Cliente, inclusa, tra l'altro, l'archiviazione o la pubblicazione su Internet di dati o contenuti diffamatori , o che rappresenti violazioni di Diritti di Proprietà Intellettuale o di diritti di terzi; (iii) violazioni di leggi o di altra normativa in materia di protezione dei dati, inclusa la protezione dei dati personali, conseguenti al trattamento dei dati stessi effettuato dal Fornitore per conto ed in conformità alle istruzioni ricevute dal Cliente o dagli Utenti; o (iv) inosservanza del presente Contratto da parte del Cliente o di un Utente. Inoltre, il Fornitore avrà il diritto di adottare misure per impedire la pubblicazione su Internet di dati, inclusi dati personali, o contenuti vietati dalla legge, e per impedire la prosecuzione di violazioni dei diritti di terzi.

8.4 Informazioni di sicurezza

8.4.1 Il Cliente manterrà adeguate misure di sicurezza per garantire che l'accesso al Servizio rimanga entro i limiti delle disposizioni del presente Contratto. In particolare, il Cliente dovrà: (i) gestire con la dovuta diligenza e attenzione eventuali identificativi, password, username o altri dispositivi di sicurezza per l'utilizzo del Servizio; (ii) adottare le misure necessarie per garantirne la riservatezza, la sicurezza e la correttezza d'uso e per impedire che persone non autorizzate ne vengano in possesso; e (iii) garantire che ciascun account utente sia utilizzato solo dall'Utente a cui è stato assegnato. Il Cliente è responsabile di tutte le attività svolte tramite le chiavi di accesso al Servizio assegnate al Cliente e agli Utenti e si impegna ad informare tempestivamente il Fornitore qualora venga a conoscenza di utilizzi non autorizzati del Servizio o di altre violazioni della sicurezza.

8.4.2 - Il Cliente, a seguito di un incidente di sicurezza informatica, deve richiedere l'intervento tramite apertura ticket (https://support.itagile.it).

8.4.3 - Il Cliente si impegna a non divulgare o a rendere disponibili a terzi le informazioni riservate conosciute o gestite in relazione all'esecuzione e/o all'esecuzione del contratto in assenza di specifico consenso scritto del Fornitore.

8.5 Obblighi del cliente

8.5.1 Il Cliente avrà i seguenti obblighi: (i) impedire interferenze da parte degli Utenti o di terzi con il Servizio; (ii) assicurarsi che i sistemi del Cliente siano adeguatamente configurati e mantenuti aggiornati per l'utilizzo del Servizio e che abbiano un adeguato accesso a Internet; (iii) informare tempestivamente il Fornitore in modo tempestivo e circostanziato in caso di problemi con il Servizio e in caso di variazione dei contatti designati dal Cliente; (iv) utilizzare e mantenere un software efficace e aggiornato per la ricerca, il rilevamento e la rimozione di malware e minacce simili; e (v) svolgere tutte le attività amministrative delle risorse umane relative al Servizio, e altre attività di competenza del Cliente, tra cui, a titolo esemplificativo: la creazione, rimozione e gestione delle chiavi di accesso (account utente) create successivamente alla predisposizione iniziale del Servizio ; l'uso operativo del Servizio da parte dei soli utenti; (vi) l'assicurazione che eventuali chiavi di accesso messe a disposizione di terzi fornitori siano immediatamente disattivate al termine dei loro servizi al Cliente; (vii) l'esecuzione delle operazioni di caricamento dei dati e delle altre operazioni e processi di gestione relativi ai dati del cliente (inclusi tutti i dati e le relative modifiche, la loro convalida e la revisione dei dati e delle relative modifiche); (viii) l'analisi delle cause dei messaggi di errore generati dalle interfacce dati e l'eventuale correzione dei dati del cliente; e lo sviluppo e l'implementazione di adeguati standard di sicurezza, procedure, autorizzazioni e controlli in relazione all'utilizzo del Servizio da parte del cliente.

9 SUPPORTO E MANUTENZIONE

9.1 Monitoraggio delle prestazioni

Il Fornitore monitora regolarmente le prestazioni del servizio con strumenti automatici e personale qualificato.

9.2 Manutenzione di emergenza.

Il Fornitore, se possibile, avviserà il Cliente via e-mail con un preavviso di almeno due ore lavorative prima di eseguire interventi di manutenzione straordinaria (es. manutenzioni, aggiornamenti, riparazioni hardware e software finalizzati alla soluzione immediata di problemi che causano instabilità nel il servizio). Tuttavia, se necessario, il lavoro può iniziare in qualsiasi momento e continuare fino al suo completamento se l'operazione non causa un degrado significativo all'ambiente specifico del Cliente e/o è altrimenti necessario o appropriato per la manutenzione complessiva o il miglioramento di funzionalità, la sicurezza o le prestazioni del Servizio. Il Fornitore adotterà tutte le misure necessarie per ridurre al minimo l'impatto sul servizio fornito al cliente durante le attività di manutenzione di emergenza.

9.3 Aggiornamenti.

Il Fornitore può, a sua discrezione, applicare aggiornamenti periodici al Servizio per migliorarne la funzionalità, la sicurezza e/o le prestazioni. Quando il Fornitore rende disponibili nuove Componenti del Servizio, il Cliente sarà libero di scegliere se acquistare nuovi prodotti in base ai Corrispettivi o alle tariffe dei Corrispettivi Contrattuali proposti dal Fornitore qualora si rendessero disponibili.

9.4 Servizi di supporto

Il Fornitore metterà a disposizione del Cliente i servizi di assistenza standard in relazione alla manutenzione e al funzionamento del Servizio. Il Fornitore fornirà servizi di supporto tramite sistema di ticketing (https://support.itagile.it); le policy di supporto prevedono l'indicazione dei tempi di risposta in base ai diversi livelli di severità delle richieste, e relative procedure di "escalation". Le richieste del Cliente che esulano dall'ambito dei servizi di assistenza standard possono essere fornite, se concordato tra il Cliente e il Fornitore, come prestazioni professionali.

9.5 Servizi professionali

Eventuali Servizi Professionali che il Fornitore potrà fornire al Cliente, su richiesta, sono forniti come servizio separato dalla fornitura del Servizio o di un Componente, alle tariffe concordate tra le parti. Se ordinati unitamente al Contratto di servizio o separatamente, i Servizi professionali sono considerati al di fuori dell'ambito di applicazione del presente Contratto e qualsiasi disaccordo o controversia relativa ai Servizi professionali non pregiudica i diritti e gli obblighi derivanti dal presente Contratto in merito alla fornitura e all'utilizzo del Servizio.

10 SOSPENSIONE DEL SERVIZIO

Il Fornitore si riserva il diritto di sospendere il servizio in caso di inadempienza del cliente o per cause di forza maggiore.

11 CLAUSOLA RISOLUTIVA ESPRESSA – RISOLUZIONE PER INADEMPIENZA – CONDIZIONI RISOLUTIVE

Il Fornitore si riserva il diritto di risolvere il contratto se il Cliente è inadempiente su qualsiasi elemento del presente contratto, e/o se espressamente previsto nell'offerta o in specifici contratti accessori all'ordine del Cliente.

12 RITIRO

Il Cliente può esercitare il recesso dal contratto solo se espressamente previsto nell'offerta commerciale o in contratti accessori all'ordine del Cliente.

13 MODIFICHE DEL CONTRATTO E/O DELLE POLITICHE DEL FORNITORE

Qualsiasi modifica al presente Contratto deve essere in forma scritta e firmata elettronicamente dalle parti. Non vi è alcun obbligo di comunicare modifiche alle politiche del Fornitore se tali modifiche non incidono sui servizi forniti.

14 COPYRIGHT E LICENZE

Tutte le componenti del servizio oggetto del contratto restano di esclusiva proprietà intellettuale del Fornitore e dei suoi eventuali subappaltatori. Il Fornitore garantisce che il servizio fornito è libero da diritti d'autore e licenze di terzi che possano in qualsiasi modo pregiudicare il Cliente.

15 INFORMAZIONI DI SICUREZZA

15.1 Sospensione del servizio

Il Fornitore può sospendere l'accesso al servizio o a parte di esso se, a discrezione del Fornitore da esercitarsi ragionevolmente, vi è il rischio che le azioni del Cliente o di un Utente compromettano l'integrità o la sicurezza del Servizio.

15.2 Segregazione di rete

Il Fornitore assicura la segregazione delle reti tra la propria rete e quella dei subappaltatori.

15.3 Rapporto sull'incidente di sicurezza

Il Fornitore segnalerà gli incidenti di sicurezza delle informazioni al Cliente utilizzando il contatto principale fornito dal Cliente. Le segnalazioni al Cliente di incidenti di sicurezza informatica avverranno entro 48 ore dal momento in cui il Fornitore ne viene a conoscenza includendo nelle comunicazioni le azioni intraprese dal Fornitore e/o eventuali azioni necessarie per la risoluzione dell'incidente da parte del Cliente.

15.4 Subappaltatori

Il Fornitore informerà il Cliente di eventuali incidenti di sicurezza informatica che si sono verificati presso i subappaltatori utilizzando il contatto principale fornito dal Cliente.

15.5 Rilevamento delle vulnerabilità

Il Fornitore svolge costantemente attività di controllo del Servizio per la rilevazione di eventuali vulnerabilità tecniche secondo i controlli previsti dalla Uni CEI EN ISO/IEC 27001:2017.

16 DENUNCE, CONTESTAZIONI

I reclami devono essere preventivamente comunicati al Fornitore attraverso l'apertura di una richiesta di supporto (ticket) come definito nel presente contratto.

17 TRATTAMENTO DEI DATI PERSONALI

17.1 GDPR

Ciascuna parte si impegna a rispettare gli obblighi derivanti dalla normativa applicabile in materia di protezione dei dati personali con riferimento al Regolamento UE 2016/679 del 27 aprile 2016 (GDPR) e al decreto legislativo 10 agosto 2018 n. 101.

17.2 Titolare del trattamento e responsabile del trattamento

Nella misura in cui i dati personali vengono trattati durante l'utilizzo del Servizio, le parti convengono che il Fornitore agisca in qualità di responsabile del trattamento nominato dal Cliente in qualità di titolare del trattamento dei dati. A tal fine, le parti si impegnano a rispettare i propri obblighi di legge in materia di protezione dei dati personali (Rif. 19.1). Il Fornitore tratterà e conserverà tali dati personali solo in nome e per conto del Cliente.

17.3 Limiti al trattamento dei dati

I dati del Cliente saranno trattati esclusivamente per le finalità del Servizio erogato dal Fornitore e per l'aggiornamento del Servizio.

17.4 Dati personali

Il Cliente è tenuto ad accertare e garantisce che i dati personali comunicati e/o forniti al Fornitore siano stati ottenuti in conformità alla normativa applicabile in materia (Rif. 19.1). Il Cliente otterrà ogni necessario consenso delle persone i cui dati sono trattati ed effettuerà le registrazioni necessarie presso le autorità competenti per consentire al Fornitore di trasferire i dati personali a terzi e per consentire al Fornitore di adempiere agli obblighi derivanti dal presente contratto.

17.5 Protezione dei dati di terze parti

Qualora un terzo dichiari una violazione dei suoi diritti in materia di protezione dei dati personali relativi allo svolgimento del Servizio, il Fornitore avrà il diritto di adottare tutte le misure che riterrà necessarie per evitare che tale violazione prosegua.

17.6 Obblighi del responsabile del trattamento

Il Fornitore dichiara espressamente di: (i) agire esclusivamente in qualità di responsabile del trattamento; (ii) adotta, al pari dei suoi fornitori e dei soggetti ospitanti, adeguate misure di sicurezza tecniche e organizzative per la protezione dei dati personali; (iii) declina ogni responsabilità in caso di trattamento dei dati personali da parte del Cliente non conforme alla normativa di cui al Rif. (19.1), con riferimento non esclusivo alla liceità del trattamento, alla corretta informativa e consenso, all'esercizio dei diritti degli interessati, ecc.

17.7 Richieste di comunicazione dei dati

Qualora il Fornitore riceva dalle forze dell'ordine una richiesta di comunicazione dei dati personali del cliente, la comunicazione dei dati personali sarà tempestivamente comunicata al referente principale dello stesso, salvo espresso divieto di legge. In ogni caso, qualsiasi comunicazione di dati personali che non sia legalmente vincolante verrà rifiutata.

17.8 Responsabile della protezione dei dati

Il Fornitore ha nominato al proprio interno un responsabile della protezione dei dati personali, dedicato alla gestione delle tematiche privacy. Il responsabile della protezione dei dati è il punto di contatto per il trattamento dei dati personali e può essere contattato utilizzando il servizio di supporto.

17.9 Violazione dei dati

Il Fornitore notificherà tempestivamente al Cliente incidenti di sicurezza o accesso non autorizzato ai dati personali del cliente (Data Breach), anche se riceve tale notifica dal subappaltatore, utilizzando il contatto principale fornito dal Cliente. Verranno fornite tutte le informazioni previste dal Regolamento UE 2016/679 del 27 aprile 2016 (GDPR).

18 LEGGE APPLICABILE E FORO COMPETENTE

Il rapporto di fornitura è regolato dalle leggi dello stato italiano. Qualsiasi controversia derivante dal – o connessa al – presente contratto, ivi comprese quelle relative alla sua validità, interpretazione, esecuzione o risoluzione, dovrà essere preventivamente sottoposta a procedimento di mediazione presso l'Istituto Nazionale per la Mediazione e l'Arbitrato. In caso di contenzioso, l'unica lingua processuale sarà l'italiano. In ogni caso le parti riconoscono la competenza esclusiva e sussidiaria del Foro di Roma (IT).

19 NOMINA A RESPONSABILE DEL TRATTAMENTO

I dati personali forniti dal Cliente al Fornitore non sono dati sensibili e sono tutelati dal Regolamento UE 2016/679 (GDPR). Il cliente acconsente all'utilizzo dei dati personali da parte di itAgile esclusivamente ai fini dell'esecuzione del presente contratto.

20 MISURE TECNICHE

Misure tecniche adottate dal Fornitore per la protezione dei dati.

20.1 Firewall

I dati personali sono protetti dal rischio di intrusione attraverso sistemi firewall, mantenuti aggiornati in relazione alle migliori tecnologie disponibili.

20.2 Protezione dai malware

I sistemi sono protetti dai malware utilizzando anti-malware aggiornati.

20.3 Credenziali di autenticazione

I sistemi sono configurati in modo da consentire l'accesso solo a soggetti muniti di credenziali univoche di autenticazione (username, password e OTP).

20.4 Parola d'ordine

La password ha le seguenti caratteristiche di base: obbligo di modifica al primo accesso, lunghezza minima otto caratteri, regole di complessità, scadenza, cronologia, valutazione contestuale della robustezza, memorizzazione hash.

20.5 Registrazione

I sistemi sono configurati in modo da consentire la tracciabilità degli accessi e, ove opportuno, delle attività svolte in capo alle diverse tipologie di utenti e protetti da adeguate misure di sicurezza che ne garantiscono l'integrità, la riservatezza e la disponibilità. Il Fornitore, ove richiesto, mette a disposizione dei clienti i log delle applicazioni da questi prodotti nell'utilizzo dei servizi dati relativi al solo richiedente.

20.6 Ripristino del backup

Sono adottate misure adeguate a garantire il ripristino dell'accesso ai dati in caso di danneggiamento dei dati o degli strumenti elettronici. Viene messo in atto un piano di business continuity e disaster recovery; assicurano la disponibilità e l'accesso ai sistemi anche in caso di eventi avversi rilevanti.

20.7 Valutazione della vulnerabilità e test di penetrazione

Il Fornitore svolge periodicamente attività di analisi delle vulnerabilità tecniche e rileva lo stato di esposizione alle vulnerabilità note, sia in relazione alle infrastrutture che agli ambiti applicativi. Ove ritenuto opportuno in relazione ai potenziali rischi individuati, tali verifiche sono periodicamente integrate con Penetration Test, attraverso simulazioni di intrusione utilizzando diversi scenari di attacco. I risultati dei controlli vengono regolarmente e approfonditamente esaminati per identificare e attuare i miglioramenti necessari per garantire il livello di sicurezza previsto.

20.8 Amministratori di sistema

Tutti gli utenti che operano in qualità di Amministratori di Sistema sono nominati con appositi atti che ne definiscono le funzioni. La loro attività viene correttamente registrata consentendo il monitoraggio tempestivo delle loro attività. La conservazione di tali dati in modo inalterabile consente un sicuro monitoraggio ex post.

20.9 Banca dati

L'accesso fisico ai Data Center utilizzati dal Servizio è limitato ai soli soggetti autorizzati. I dettagli delle misure di sicurezza di questi Data Center sono disponibili sui relativi siti istituzionali.

20.10 Sicurezza delle comunicazioni

Protocolli di comunicazione sicuri sono adottati dal Fornitore ed in linea con quanto la tecnologia mette a disposizione. I flussi di dati da e verso i sistemi cloud esposti su Internet sono protetti utilizzando un canale TLS sicuro per garantire:

- Autenticazione del server (chiave RSA a 2048 bit)

- Crittografia di sessione con algoritmo di crittografia simmetrica, considerata ragionevolmente sicura alla data, con una chiave di sessione di almeno 128 bit

20.11 Crittografia

Il Fornitore adotta le più recenti tecniche di cifratura sui dati presenti nei database per renderli inutilizzabili a chi non è autorizzato a visionarli. La crittografia viene applicata anche nelle comunicazioni da e verso i sistemi dei fornitori.

20.12 Hardening

Sono in atto speciali attività di hardening per prevenire il verificarsi di eventi avversi minimizzando le debolezze architetturali di sistemi operativi, applicazioni e apparati di rete.

20.13 Cancellazione sicura di dati e file temporanei

Il Fornitore assicura che lo spazio su disco messo a disposizione dei clienti sia pulito prima dell'uso attraverso una procedura di cancellazione sicura eseguita al termine del servizio.

20.14 Orologio di Sincronizzazione

Tutti i sistemi cloud del fornitore utilizzano il protocollo NTP per la sincronizzazione dell'orologio. La fonte dell'orologio è INRIM (www.inrim.it). Il fuso orario utilizzato è CET/CEST.

20.15 Sviluppo sicuro

L'ambiente di sviluppo del software è accessibile solo al personale addetto alla codifica e al test. Il processo di sviluppo del Fornitore segue linee guida di sviluppo sicuro volte a garantire il rispetto dei principi di Security by Design. Il test del codice segue un processo predefinito per valutare sia la funzionalità del codice che la presenza di gravi vulnerabilità. Il passaggio alla produzione avviene manualmente e le modifiche sono opportunamente tracciate. Gli ambienti di sviluppo, test e produzione sono logicamente separati.

21 MISURE ORGANIZZATIVE

Misure organizzative del fornitore per la protezione dei dati trattati nel Servizio.

21.1 Politiche e regolamenti

Il Fornitore applica norme che tutti gli utenti che hanno accesso a sistemi informativi hanno l'obbligo di rispettare, volte a garantire comportamenti idonei ad assicurare la protezione dei dati nell'utilizzo delle risorse informatiche.

21.2 Accesso logico

Il Fornitore definisce i profili di accesso nel rispetto dei *principi del minimo privilegio* e della *necessità di conoscere necessari per* l'esecuzione degli incarichi assegnati. Tali profili sono soggetti a controlli periodici.

21.3 Supporto alla gestione delle operazioni

Le operazioni di supporto garantiscono la corretta esecuzione del Servizio evitando l'eccessivo trattamento di dati personali la cui titolarità o responsabilità è del Cliente o dell'Utente Finale.

21.4 Gestione degli incidenti

Il Fornitore ha implementato una procedura per la gestione degli incidenti informatici per assicurare il ripristino della normale operatività del servizio nel più breve tempo possibile, assicurando il mantenimento dei livelli di servizio.

21.5 Gestione delle violazioni dei dati

Il Fornitore ha implementato una procedura per la gestione della violazione dei dati personali. Tale procedura definisce ruoli e responsabilità, tempi e modalità di comunicazione all'interessato e all'autorità di controllo.

21.6 Formazione

Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nella gestione dei servizi, corsi sulla sicurezza delle informazioni e sulla corretta gestione dei dati personali.

21.7 Gestione del cambiamento

Il Fornitore dispone di una specifica procedura di gestione del cambiamento per l'introduzione di eventuali innovazioni tecnologiche o modifiche del proprio approccio e della propria struttura organizzativa.

21.8 Audit interno

Il Fornitore affida a personale esterno qualificato l'esecuzione di audit interni sulla sicurezza delle informazioni di qualità, business continuity e privacy; la periodicità di tali attività è specificata nel programma annuale di audit.

21.9 Certificazioni

il Fornitore ha ottenuto le certificazioni per il campo di applicazione "erogazione e gestione di servizi di firma digitale remota" secondo i seguenti standard internazionali:

- UNI CEI EN ISO/IEC 27001:2017
- ISO/IEC 27017:2015
- ISO/IEC 27018:2019
- UNI EN ISO 9001:2015

21.10 LIMITAZIONI ALL'UTILIZZO DEL SERVIZIO

Il mancato rispetto da parte del Cliente delle seguenti condizioni comporterà l'immediata sospensione del Servizio. Per qualsiasi richiesta di chiarimento in merito alle Condizioni Generali il cliente può aprire un ticket all'indirizzo https://support.itagile.it

21.11 Violazioni

L'utilizzo del servizio di firma remota per attività illecite, ad insindacabile giudizio del Fornitore, comporta la cessazione del servizio. Le credenziali per accedere al servizio sono strettamente personali e non cedibili a terzi. Di seguito sono riportati esempi di attività vietate:

- Cessione delle credenziali di accesso a terzi
- Accesso (o utilizzo) non autorizzato
- Negazione del servizio
- Test di carico/prestazioni

21.12 Prove di vulnerabilità

Qualsiasi attività di Vulnerability Assessment e Penetration Test deve essere preventivamente autorizzata dal Fornitore. L'esecuzione senza consenso scritto può comportare, a discrezione del Fornitore, la cessazione del servizio.