CAPITOLATO TECNICO

ACQUISIZIONE SISTEMA GESTIONALE LEGALE E SERVIZI CONNESSI

INDICE

1 PREMESSA

Beneficiaria del servizio è la Divisione Affari Legali, che cura la difesa giudiziale dell'azienda, gestendo in particolare i rapporti con l'Avvocatura dello Stato (titolare della rappresentanza e della difesa in giudizio della Consip nell'ambito del Programma di razionalizzazione degli acquisti della Pubblica Amministrazione, ai sensi dell'art.1 comma 771 della L. 145/2018), e con gli avvocati del libero foro (per gli altri giudizi).

La struttura legale per gestire in termini amministrativi le suddette attività utilizza attualmente la Suite "Ufficio Legale" (opportunamente personalizzata per gestire le peculiarità delle procedure operative legate ai contenziosi della Consip), di cui la soluzione "SuiteNext", oggetto della presente acquisizione, è l'evoluzione SAAS.

Si riepilogano di seguito le peculiarità di tale applicativo:

- dispone dei termini processuali aggiornati, al fine di scadenzare tutti gli adempimenti processuali, e quindi poter coinvolgere tempestivamente le strutture aziendali impattate dal contenzioso, onde reperire le informazioni e i documenti necessari per la difesa in giudizio e dare riscontro, nel rispetto delle scadenze processuali, ai difensori esterni;
- fornisce una reportistica in grado di gestire un ingente numero di contenziosi pari solo ad alcune delle società partecipate che del pari utilizzano il medesimo applicativo;
- consente la creazione di schede specifiche in cui sono gestiti numerosi campi informativi (es. lotti delle gare, richiesta di risarcimento danni ed eventuale quantificazione, motivo principale del ricorso, thema decidendum, presenza di fase cautelare ed esito, nome dell'estensore della sentenza/ordinanza);
- gestisce riferimenti comuni con l'Avvocatura dello Stato (che rappresentano la maggioranza dei contenziosi), agevolando la gestione dei fascicoli Consip con le corrispondenti pratiche dell'Avvocatura dello Stato;
- generazione del fascicolo elettronico per ciascuna pratica, gestione agenda legale e integrazione servizi posta e messaggistica (ad es. remind su calendario del Personal Information Manager (PIM) Consip es. outlook o altro strumento di posta), presenza di un archivio documentale, generazione di cruscotti e report, ecc inoltre funzioni per amministratore di sistema e gestione dei log;
- disponibilità di protocolli standard per integrazione con sistemi esterni;
- profilazione utenti in ragione dei differenti ruoli aziendali: admin, utente in scrittura, utente in lettura);
- soluzione SaaS qualificata dall'Agenzia per la Cybersicurezza Nazionale.

2 OGGETTO E DURATA

Oggetto dell'affidamento è l'acquisizione del sistema gestionale legale SuiteNext e dei servizi connessi secondo il seguente dettaglio:

Descrizione	Quantità
Subscription	6 utenti
Supporto professionale (a consumo)	18 giornate

Costituisce parte integrante e sostanziale del Contratto il documento “Allegato A | DOCUMENTO DI SLA (service level agreement)” allegato al presente capitolato tecnico.

Il contratto avrà durata pari a 24 mesi a partire dalla “Data di avvio del servizio”.

3 DESCRIZIONE DEL SERVIZIO

3.1 FORNITURA LICENZE

Il Fornitore dovrà garantire l’accesso all’applicativo per un numero di 6 (sei) utenze nominali.

L’applicativo fornito dovrà garantire la continuità del servizio erogato attualmente, mantenendo dati e personalizzazioni realizzate nella precedente fornitura.

Il servizio viene erogato tramite un’infrastruttura cloud SaaS, i cui requisiti sono dettagliati nell’allegato al presente Capitolato Tecnico “Allegato A | DOCUMENTO DI SLA (service level agreement)”.

3.2 SUPPORTO PROFESSIONALE PER SVILUPPI E INTEGRAZIONI

Nel corso della durata contrattuale saranno richieste 18 giornate di servizi professionali per consentire: indicazioni su roadmap evolutiva del prodotto;

- sviluppo di eventuali customizzazioni e integrazioni con altre applicazioni.

Per ciascun intervento richiesto il Fornitore, in base alla specifica esigenza, indicherà l’impegno stimato in termini di giornate, che sarà sottoposto all’approvazione da parte di Consip. La consuntivazione delle attività svolte avverrà al termine dell’intervento e della consegna degli output richiesti.

4 MODALITÀ DI EROGAZIONE DEL SERVIZIO

Si faccia riferimento all’allegato “Allegato A | DOCUMENTO DI SLA (service level agreement)”.

5 ASSISTENZA, HELP DESK E AGGIORNAMENTI

Si faccia riferimento all’allegato “Allegato A | DOCUMENTO DI SLA (service level agreement)”.

6 LIVELLI DI SERVIZIO

Si faccia riferimento all’allegato “Allegato A | DOCUMENTO DI SLA (service level agreement)”.

7 RESPONSABILE DELLE ATTIVITÀ

Il Fornitore dovrà comunicare, entro 5 (cinque) giorni lavorativi dalla stipula del contratto, il nominativo del proprio rappresentante, designato quale Responsabile delle attività. Il Fornitore deve provvedere in piena autonomia al coordinamento e all’organizzazione delle attività nel rispetto delle specifiche e dei tempi forniti

da Consip S.p.A. Sarà compito del Responsabile del servizio curare la gestione amministrativa del contratto e delle attività legate alla fatturazione e verificare il rispetto di tutti gli adempimenti contrattuali.

8 MODALITÀ DI COMUNICAZIONE

Il Fornitore si impegna a comunicare, contestualmente alla stipula del contratto, un indirizzo e-mail e un numero di telefono al quale rivolgersi per ogni comunicazione relativa alle attività, nonché i riferimenti specifici (telefonico, via mail, ecc.) per il servizio di help desk.
Resta inteso che, per tutta la durata contrattuale, il Fornitore dovrà garantire la piena funzionalità dei suddetti mezzi di comunicazione comunicando tempestivamente a Consip S.p.A. eventuali modifiche.

9 ADEMPIMENTI PER LA SICUREZZA

Il Fornitore si impegna a porre in essere quanto necessario per garantire l'esecuzione delle attività in piena aderenza con le disposizioni del D.Lgs. 81/2008 s.m.i., cooperando e coordinandosi, in particolare, con i referenti di Consip, ai fini degli adempimenti di cui all'art. 26 del citato decreto.

10 MODALITÀ DI FATTURAZIONE E PAGAMENTO

Per la fatturazione delle licenze (Subscription) di cui al par. 3.1, si applica quanto previsto al paragrafo 15, comma 1 delle Condizioni particolari: "*Ai fini del pagamento del corrispettivo indicato nel presente contratto per la fornitura di beni, da intendersi inclusivo del servizio di manutenzione in garanzia, il Fornitore potrà emettere fattura successivamente al certificato di verifica di conformità positivo*".

Per la fatturazione del Servizio di supporto professionale di cui al par. 3.2, si applica quanto previsto al paragrafo 15, comma 3 delle Condizioni particolari: "*Ai fini del pagamento del corrispettivo indicato nel presente contratto, il Fornitore potrà emettere fattura successivamente alla approvazione da parte della Committente del "consuntivo attività", contenente il dettaglio delle prestazioni erogate nel periodo di riferimento, nonché della verifica di conformità positiva. Nella fattura dovrà essere indicato il periodo temporale di riferimento.*"
Le fatture dovranno essere emesse sulla base del numero di giorni effettivamente erogati al termine del trimestre solare di riferimento, ovvero alla data del 31 marzo, 30 giugno, 30 settembre e 31 dicembre.

Il pagamento del corrispettivo verrà effettuato dalla Consip secondo le modalità di cui alla vigente normativa e in coerenza con quanto previsto dalle Condizioni contrattuali.

11 PENALI

Le penali previste sono riportate nell'art.13 delle Condizioni Contrattuali.

Allegati:

"Allegato A | DOCUMENTO DI SLA (service level agreement)"

Wolters Kluwer Italia S.r.l.
Via Dei Missaglia, n. 97
Edificio B3
20142 Milano (MI)
Tel. +39 02 824761
Fax +39 02 82476799

S.r.l. a Socio Unico
Dir. Coord. di Wolters Kluwer N.V.
Capitale sociale: € 19.640.000 int. vers.
R. Imprese di Milano, Codice Fiscale
e Partita IVA 10209790152
R.E.A. di Milano N. 1353036

Allegato A | DOCUMENTO DI SLA (Service Level Agreement)

Sommario

Wolters Kluwer Italia S.r.l.
Via Dei Missaglia, n. 97
Edificio B3
20142 Milano (MI)
Tel. +39 02 824761
Fax +39 02 82476799

S.r.l. a Socio Unico
Dir. Coord. di Wolters Kluwer N.V.
Capitale sociale: € 19.640.000 int. vers.
R. Imprese di Milano, Codice Fiscale
e Partita IVA 10209790152
R.E.A. di Milano N. 1353036

1. Introduzione

Wolters Kluwer Italia S.r.l. (di seguito anche "WKI") ha sviluppato una soluzione innovativa per l'erogazione del proprio applicativo in modalità web, ovvero su piattaforma cloud con alti livelli di affidabilità, sicurezza e scalabilità.

2. Descrizione del servizio

Il servizio viene erogato tramite un'infrastruttura basata sulla piattaforma cloud Azure di Microsoft, che garantisce elevati livelli di servizio in merito a:

- Sicurezza fisica dei server
- Protezione da interruzioni di alimentazione
- Ridondanze di apparati
- Banda con profilo dinamico
- Duplicazione delle istanze applicative e dei dati su base geografica.

Rimane facoltà di WKI, in qualsiasi momento della durata del Contratto, di cambiare il soggetto titolare dell'infrastruttura, senza previo avviso al Cliente, garantendo comunque a quest'ultimo gli stessi SLA di Servizio di cui al presente documento.

Al fine di garantire la sicurezza del software in termini di integrità, disponibilità e riservatezza delle informazioni, l'organizzazione ha adottato un Secure Development Life Cycle (SLDC).
Il rispetto delle policy e delle procedure di sviluppo sicuro viene esteso a tutti i soggetti esterni coinvolti nelle attività si sviluppo software.
Nell'ambito del SLDC sono condotte con cadenza periodica attività di vulnerability assessment (VA) e penetration test (PT) sia a livello applicativo che infrastrutturale. In funzione del livello di impatto sul servizio offerto al Cliente vengono definiti ed attuati piani di remediation delle vulnerabilità tecniche eventualmente emerse.

3. Requisiti hardware e software:

Computer: può essere utilizzato un computer con requisiti minimi di sistema, in grado di connettersi ad internet. Sono supportati sistemi operativi sia Windows che MAC. Il browser consigliato è Chrome, sono comunque supportati i seguenti browser:

- Mozilla Firefox
- Chrome
- Opera
- Microsoft Edge
- Safari

- Linee Internet da utilizzare:

• ADSL Consumer/Business (requisito minimo) • Fibra (requisito consigliato)

4. Modalità di erogazione del servizio

Il Cliente previa verifica dell'identità, riceve, tramite due canali differenti (e-mail e telefono), la User e la relativa Chiave di Accesso (di seguito la "Chiave di Accesso **dell'utente Admin**"), tramite la quale poter attivare altri Utenti abilitati ad accedere ed utilizzare il Servizio.

Gli Utenti abilitati saranno in numero pari al numero di Utenti richiesto dal Cliente e riportato nel Modulo d'Ordine.

L'utente può essere vincolato: alla sola lettura e/o alla modifica dei dati, all'inserimento di nuovi dati e/o alla cancellazione degli stessi

4.1 Aree di memoria a disposizione del Cliente

Le aree di memoria messe a disposizione da WKI nei propri server durante l'erogazione del Servizio saranno utilizzate in modo automatico solo per la memorizzazione dei dati degli adempimenti del cliente. È fatto divieto a quest'ultimo di utilizzare le predette aree per memorizzare altre informazioni o per altri scopi.

4.2 Accesso al servizio SaaS

Il cliente può accede al servizio in due modalità:

1) accesso standard tramite l'indirizzo https://portal.suitenext.com, se non diversamente indicato nella proposta d'ordine
2) accesso personalizzato https://<cliente>.suitenext.com, se espressamente indicato nella proposta d'ordine.

L'accesso, in entrambi i casi, è regolato da utente e password.

5. SLA relativo alla Infrastruttura

Wolters Kluwer Italia S.r.l. ha definito con Microsoft i livelli di servizio della piattaforma cloud Microsoft Azure.
Si fa pertanto riferimento alle garanzie che Microsoft stessa presta, di cui si riportano le caratteristiche più significative.

5.1 Protezione per l'ambiente di hosting

L'ambiente della piattaforma Microsoft Azure è costituito da computer, sistemi operativi, applicazioni e servizi, reti, apparecchiature per le operazioni e il monitoraggio e hardware specializzato, oltre dagli operatori e dal personale amministrativo necessari per eseguire e gestire i servizi. L'ambiente include, inoltre, centri operativi fisici che ospitano i servizi e che richiedono protezione da eventuali danni intenzionali e accidentali.

Punti di progettazione architetturale principali

La piattaforma Microsoft Azure è progettata per fornire una "difesa in profondità" e ridurre il rischio che il guasto di un singolo meccanismo di protezione comprometta la sicurezza dell'intero ambiente. I livelli di difesa in profondità includono:

- Router di filtraggio: i router di filtraggio respingono i tentativi di comunicazione tra indirizzi e porte non configurati nel modo consentito. Questa soluzione consente di

prevenire gli attacchi più comuni che utilizzano "droni" o "zombie" per la ricerca di server vulnerabili. Benché siano relativamente facili da bloccare, questi tipi di attacchi restano il metodo preferito dagli utenti malintenzionati in cerca di vulnerabilità. I router di filtraggio supportano, inoltre, la configurazione dei servizi back-end in modo che siano accessibili solo dai corrispondenti front-end.

- Firewall: i firewall limitano le comunicazioni di dati da e verso porte, protocolli e indirizzi IP di destinazione (e di origine) noti e autorizzati.
- Gestione delle patch di protezione del software: la gestione delle patch di protezione costituisce parte integrante delle operazioni che garantiscono la protezione dei sistemi dalle vulnerabilità note.
  La piattaforma Windows Azure utilizza sistemi di distribuzione integrati per gestire la distribuzione e l'installazione delle patch di protezione per il software Microsoft.
- Monitoraggio: la protezione viene monitorata con l'ausilio di sistemi di monitoraggio, correlazione e analisi centralizzati in grado di gestire l'elevato volume di informazioni generato dai dispositivi all'interno dell'ambiente, fornendo monitoraggio e avvisi pertinenti e tempestivi sul superamento soglie (CPU, RAM e spazio disco), creando automaticamente degli incident a seguito di down.
- Segmentazione di rete: Microsoft utilizza diverse tecnologie per creare barriere contro il traffico non autorizzato in corrispondenza dei principali punti di giunzione verso i data center e al loro interno, tra cui firewall, caselle NAT (Network Address Translation) (bilanciamento del carico) e router di filtraggio. La rete di back-end è costituita da reti locali (LAN) partizionate per server applicazioni e Web, archiviazione dei dati e amministrazione centralizzata. Tali server sono raggruppati in segmenti di indirizzi privati protetti da router di filtraggio.

5.2 Protezione fisica

La protezione fisica va di pari passo con le misure di protezione basate sul software e a entrambe si applicano analoghe procedure di valutazione e attenuazione dei rischi.
I servizi della piattaforma Microsoft Azure vengono forniti ai clienti attraverso una rete di data center, progettati per l'esecuzione 24 ore su 24, 7 giorni su 7 e per l'utilizzo di diverse misure per proteggere le operazioni da eventuali interruzioni di alimentazione, intrusioni fisiche e interruzioni della rete. Questi data center sono conformi agli standard del settore relativi a protezione fisica e affidabilità, vengono gestiti, monitorati e amministrati da operatori Microsoft e sono situati in località geografiche diverse.
Per SuiteNext il sito primario (produzione) è nella regione West Europe, il sito secondario (DR) è nella regione North Europe. Per ulteriori dettagli sulla localizzazione dei siti, si rimanda al seguente link messo a disposizione da Microsoft. https://azure.microsoft.com/it-it/global-infrastructure/geographies/
Microsoft utilizza meccanismi di accesso altamente protetti, limitati a un numero molto ristretto di propri operatori ed operatori WKI che sono tenuti a modificare regolarmente le proprie password di accesso amministratore. L'accesso ai data center e l'autorizzazione ad aprire i ticket di accesso per i data center vengono sottoposti al controllo del responsabile delle operazioni di rete, nel rispetto delle procedure di protezione dei data center locali.
WKI si è dotata di un sistema di log management centralizzato per il tracciamento degli accessi (login e logout) WKI archivia tali log per un periodo non inferiore ai sei mesi, avendo

cura di salvaguardare la loro integrità. WKI potrà rendere disponibili i log al Cliente in caso di specifica richiesta puntuale.

Per garantire la riservatezza dei dati in transito il servizio fornito si avvale di protocolli di comunicazione sicura basati su certificati (HTTPS, FTPS, SFTP). Gli standard utilizzati vengono periodicamente riesaminati e aggiornati in funzione dell'evoluzione tecnologica.

La configurazione NTP Clock Synchronization) dei sistemi utilizzati per l'erogazione dei servizi si basa sul servizio messo a disposizione da Microsoft Azure.

Per l'erogazione del servizio, viene effettuata la sincronizzazione degli orologi di sistema usando i servizi nativi di Azure.

5.3 Protezione delle operazioni e del personale

Progettazione dei servizi

La piattaforma Microsoft Azure è progettata per l'esecuzione senza accesso di routine ai dati dei clienti da parte del personale Microsoft; solo un numero limitato di operatori può accedere alle informazioni dei clienti.

Risposta agli eventi imprevisti

I servizi della piattaforma Microsoft Azure dispongono di operatori che lavorano 24 ore al giorno, 7 giorni su 7. Se l'evento imprevisto è legato alla protezione, le procedure documentate da seguire vengono implementate dal personale addetto. È inoltre disponibile un piano di comunicazione completo che viene implementato nel caso di un evento imprevisto legato alla protezione.

5.4 Tolleranza di errore e ridondanza

La piattaforma Microsoft Azure è progettata per garantire tolleranza di errore e ridondanza. Ogni livello dell'infrastruttura della piattaforma Microsoft Azure è progettato per consentire il proseguimento delle operazioni in caso di errore, inclusi dispositivi di rete ridondanti a ogni livello e doppi provider di servizi Internet in ciascun data center. Il failover avviene nella maggior parte dei casi in modo automatico, senza necessità di intervento umano, e la rete viene monitorata dal Network Operations Center (NOC) 24 ore al giorno, 7 giorni su 7, per rilevare eventuali anomalie o potenziali problemi di rete.
L'alta affidabilità è ulteriormente garantita da una coppia di server ridondati.

5.5 Capacity Plan

Il dimensionamento dell'infrastruttura viene garantito attraverso un monitoraggio costante delle metriche di utilizzo (CPU, RAM, Spazio disco) e scalando l'infrastruttura di conseguenza.

5.6 Spazio di archiviazione sull'infrastruttura

Ogni cliente, con configurazione standard, dispone all'interno della piattaforma di uno storage pari a 50GB per il caricamento di dati e documenti, indipendentemente dal numero di utenti attivi, sia interni che esterni.

5.7 Servizio di Backup dell'infrastruttura

Il servizio di backup ha come obiettivo la protezione dei dati, finalizzato al ripristino degli stess in caso di cancellazione accidentale.

A richiesta, è possibile recuperare dati secondo le seguenti specifiche:

- Dati strutturati: fino a 35 gg prima
- Documenti e file allegati: fino a 35 gg prima e nei limiti dello spazio disponibile

5.8 Limiti all'utilizzo dell'infrastruttura

Il cliente non è autorizzato ad eseguire, direttamente o tramite terze parti, alcuna attività tecnicamente invasiva o di analisi sulla piattaforma o sulla sua infrastruttura, e più in generale fuori dall'utilizzo standard dell'applicativo gestionale, che possa in qualsiasi modo inficiare la sicurezza e le performance della soluzione, quali a titolo esemplificativo e non esaustivo: vulnerability assessment, penetration test, reverse engineering del codice, ethical hacking, etc.

5.9 Dati di Targa infrastruttura

Si riportano i dati di targa garantiti da Microsoft che sono alla base del servizio offerto e di cui beneficerà il cliente durante l'utilizzo del prodotto applicativo oggetto del contratto:
La disponibilità dell'infrastruttura è garantita per il 99,80% per 24 ore al giorno, 365 giorni l'anno.
Per indisponibilità s'intende una interruzione della rete sull'infrastruttura Microsoft Azure che impedisca il raggiungimento dei servizi di Wolters Kluwer Italia S.r.l. ospitati sulla piattaforma cloud Microsoft Azure da una postazione esterna per un periodo di almeno cinque (5) minuti.
Essa non include sospensioni programmate per interventi tecnici, interruzioni parziali, degrado del servizio, interruzioni dovute a catastrofi, sommosse, eventi di carattere eccezionale.

6. SLA sulle applicazioni WKI

WKI offre le proprie garanzie relativamente al funzionamento dei servizi applicativi ospitati sulla piattaforma Microsoft Azure.

Wolters Kluwer Italia S.r.l.
Via Dei Missaglia, n. 97
Edificio B3
20142 Milano (MI)
Tel. +39 02 824761
Fax +39 02 82476799

S.r.l. a Socio Unico
Dir. Coord. di Wolters Kluwer N.V.
Capitale sociale: € 19.640.000 int. vers.
R. Imprese di Milano, Codice Fiscale
e Partita IVA 10209790152
R.E.A. di Milano N. 1353036

6.1 System monitoring

I servizi sono costantemente monitorati dal personale WKI al fine di:

- Sovrintendere, senza interruzioni, al funzionamento di tutte le componenti del servizio erogato ai clienti
- Gestire l'esecuzione delle procedure operative e il mantenimento della documentazione relativa all'operatività
- Interfacciare le terze parti (es. fornitori, partner, clienti) coinvolte nel processo di erogazione e governance dei servizi.

A fronte del flusso di eventi generato dai server, gli operatori WKI applicano le procedure operative di gestione, sia generali, sia, eventualmente, specifiche per il singolo servizio.
Gli scopi del servizio di monitoraggio sono:

1. L'individuazione, preventiva o reattiva, degli eventuali problemi di funzionamento dei servizi (troubleshooting)
2. Assicurare il rispetto dei valori garantiti nel presente documento Service Level Agreement (SLA)

6.2 System management

Le componenti del Servizio Base di System Management sono:

Problem solving

- Gestione dei contratti di manutenzione con i fornitori HW/SW, relativamente alle componenti gestite, in caso di failure
- Risoluzione di eventi dei software registrati nel system-log file

Gestione ordinaria

- Tuning dei parametri prestazionali
- Segnalazione di procedure operative da notificare al cliente

Manutenzione

- Pianificazione ed esecuzione degli interventi di manutenzione ordinaria e straordinaria sulle applicazioni

6.3 Disponibilità del servizio software

- Il servizio software sarà di norma disponibile 24 ore al giorno, 365 giorni l'anno, fatta salva una FINESTRA DI MANUTENZIONE per le attività quotidiane di MANUTENZIONE ordinaria (patching, ecc).
  Questa fascia di indisponibilità del SERVIZIO SOFTWARE dovrà avere una durata non superiore ai 60 minuti, collocata nella fascia 18.00 – 08.00 e segnalata tramite apposita pagina di cortesia.
- Gli interventi di MANUTENZIONE straordinaria effettuati al di fuori della FINESTRA DI MANUTENZIONE e/o per una durata superiore ai 60 minuti saranno segnalati con 3 gg di anticipo tramite apposita pagina di cortesia.

Wolters Kluwer Italia S.r.l.
Via Dei Missaglia, n. 97
Edificio B3
20142 Milano (MI)
Tel. +39 02 824761
Fax +39 02 82476799

S.r.l. a Socio Unico
Dir. Coord. di Wolters Kluwer N.V.
Capitale sociale: € 19.640.000 int. vers.
R. Imprese di Milano, Codice Fiscale
e Partita IVA 10209790152
R.E.A. di Milano N. 1353036

6.4 Dati di targa servizio software

Nelle tabelle seguenti sono riportati i gradi di severity del "guasto" ed il relativo tempo di ripristino.
Per indisponibilità s'intende una interruzione del servizio della rete della Farm che impedisca il raggiungimento di tutti gli apparati di Wolters Kluwer Italia ospitati in Microsoft Azure da una postazione esterna per un periodo di almeno quindici (15) minuti, ma non include sospensioni programmate per interventi tecnici, interruzioni parziali, degrado del servizio, interruzioni dovute a catastrofi, sommosse, eventi di carattere eccezionale, interruzioni dei circuiti forniti da Telecom Italia o da altri carrier.

Livelli di Severity	
Emergenza	Grave indisponibilità del servizio che ha un serio impatto sulle attività del cliente e non può essere aggirata. Impossibilità di utilizzo del servizio.
Grave	Anomalie parziali a cui è possibile applicare soluzioni temporanee per garantire l'erogazione del servizio.
Normale	Inefficienze minori nel servizio che non hanno un immediato impatto sul servizio del Cliente.

Tempo di intervento	
Monitoraggio ambiente di produzione	24h al giorno tutti i giorni
Incident con priorità "Emergenza" o "Grave"	Massimo 30 min → Lunedì ÷ Venerdì 09:00 ÷ 18:00 (festivi esclusi) ---------- Massimo 1h → nell'orario rimanente
Altri incident	entro 2h → Lunedì ÷ Venerdì 09:00 ÷ 18:00 (festivi esclusi)

SLA di servizio (disponibilità infrastruttura)		
Availability	Business Hours 9/18 Mon/Fri	99,80%
	Operating Hours	99,80%
RTO	< 6 Hr (6/20 Mon/Fri) < 8 Hr (9/18 Sat) < 10.00 AM next day (in all other time)	100%
RPO	< 4 Hr	100%

Wolters Kluwer Italia S.r.l.
Via Dei Missaglia, n. 97
Edificio B3
20142 Milano (MI)
Tel. +39 02 824761
Fax +39 02 82476799

S.r.l. a Socio Unico
Dir. Coord. di Wolters Kluwer N.V.
Capitale sociale: € 19.640.000 int. vers.
R. Imprese di Milano, Codice Fiscale
e Partita IVA 10209790152
R.E.A. di Milano N. 1353036

6.5 Ruoli e responsabilità per il servizio SaaS

Attività	WKI	AZURE o TERZE PARTI	Cliente
Cifratura	A		
Monitoraggio Infrastrutturale	A/R		
Log Amministratori di Sistema (WKI)	A/R		
Log Amministratori di Sistema (Terze parti)	A/R		
Log Amministratori di Sistema Cliente	A/R		
Log Account Utenti finali	A/R		
Log Applicazioni	A/R		
Sincronizzazione dei clock di sistema	R	A	
Configurazione sicura sistemi (Lato SERVER)	A/R		
Configurazione sicura sistemi (Infrastruttura SAAS)	A/R		
Configurazione sicura sistemi (Lato Client)	A		R
Vulnerability Assessment	A/R		
Penetration Test	A	R	
Patching Client	A		R
Patching Server	A/R		
Patching infrastruttura SAAS	A/R		
Change Management (Servizio SAAS)	A/R		
Change Management (Infrastruttura Servizio SAAS)	A/R		
Capacity Management (Risorse Infrastrutturali)	A/R		
Incident Management / Data Breach	A/R	R	
Cancellazione e dismissione	A/R		I
Gestione accessi logici su ambienti virtuali e network		A	
Gestione account utenti finali per accesso ai servizi	A		C
Gestione profilazione utenti finali per accesso ai servizi	A		C
Data Center – Gestione Sicurezza fisica ed ambientale		A	
Network – Gestione connettività Data Center		A	
Network – Gestione connettività utente finale			A
Gestione Backup	A		
Gestione Antivirus su ambiente di produzione	A/C		

Wolters Kluwer Italia S.r.l.
Via Dei Missaglia, n. 97
Edificio B3
20142 Milano (MI)
Tel. +39 02 824761
Fax +39 02 82476799

S.r.l. a Socio Unico
Dir. Coord. di Wolters Kluwer N.V.
Capitale sociale: € 19.640.000 int. vers.
R. Imprese di Milano, Codice Fiscale
e Partita IVA 10209790152
R.E.A. di Milano N. 1353036

7. Modalità di erogazione dei servizi di assistenza, help-desk ed aggiornamenti

Il Cliente potrà usufruire dei Servizi di assistenza telefonica e di interventi in teleassistenza sul Programma applicativo dalle ore 09:00 alle ore 13:00 e dalle ore 15:00 alle ore 18:00, tutti i giorni ad eccezione del sabato e dei giorni festivi. I servizi di assistenza tecnica del software saranno erogati da WKI e/o dal Distributore.

3. I tempi di presa in carico della richiesta rientrano in un arco di tempo massimo di 5 giorni lavorativi, a prescindere che siano state inoltrate via telefono o tramite e-mail.

4. Il ripristino delle funzionalità a fronte di eventuali bug o malfunzionamenti prevede tempi di intervento che dipendono necessariamente dalla gravità del problema.

- malfunzionamento bloccante – (inaccessibilità di un'applicazione da parte di tutti gli utenti) – presa in carico entro 4h
- malfunzionamento non bloccante – (malfunzionamento o bug non bloccante) – presa in carico entro 5gg
- chiarimento su funzionalità applicativa – risposta entro 5gg.

8. Portabilità del dato

I dati generati in SuiteNext durante l'utilizzo del servizio sono di esclusiva proprietà del Cliente e rimangono a sua completa disposizione in ogni momento e per tutta la durata del Servizio. Ad ogni modo, WKI si impegna a notificare tempestivamente ai clienti del servizio qualsiasi richiesta legalmente vincolante di divulgazione di dati personali da parte dell'autorità giudiziaria, a meno che tale divulgazione non sia altrimenti vietata.
In caso di risoluzione del contratto, WKI restituirà al cliente, su sua richiesta, i dati memorizzati strettamente legati all'utilizzo del gestionale SuiteNext. I dati saranno consegnati in un formato di file standard, backup DB SQL server. La consegna, senza spese aggiuntive, avverrà entro 30 giorni lavorativi dal giorno di conclusione del contratto. Su richiesta del Cliente i dati si possono ottenere in altro formato, con modalità e tempi da concordare. Tutto ciò che non è espressamente riportato è a cura del cliente.
Dalla cessazione del contratto, WKI non sarà più ritenuta responsabile del servizio e nulla potrà esserle addebitato per l'interruzione dello stesso.
Entro 90 giorni dalla data effettiva di cessazione del Contratto, WKI provvederà a distruggere in modo sicuro i dati e i relativi backup.

9. Limiti di applicabilità degli SLA

Oltre alle ipotesi contrattualmente previste, sono di seguito riportate ulteriori fattispecie giustificative del mancato rispetto da parte di WKI degli SLA sopra indicati e di conseguente esclusione di responsabilità di WKI:

1. Indisponibilità delle linee d'accesso del Cliente;
2. Anomalie che comportano il blocco di una specifica funzionalità, in tale caso il Cliente sarà avvisato tramite apposita pagina di cortesia;

Wolters Kluwer Italia S.r.l.
Via Dei Missaglia, n. 97
Edificio B3
20142 Milano (MI)
Tel. +39 02 824761
Fax +39 02 82476799

S.r.l. a Socio Unico
Dir. Coord. di Wolters Kluwer N.V.
Capitale sociale: € 19.640.000 int. vers.
R. Imprese di Milano, Codice Fiscale
e Partita IVA 10209790152
R.E.A. di Milano N. 1353036

3. Inaccessibilità logica alle risorse della infrastruttura dovute a cambiamenti dei controlli di accesso fatte dal provider Microsoft e non comunicate a WKI;
4. Indisponibilità del servizio causata da azioni non direttamente imputabili a WKI;
5. Interruzioni del Servizio dovute ad indisponibilità di reti di altri provider (es: ISP di accesso dell'utente);
6. Indisponibilità del servizio Internet dovuta a disservizi sugli Upstream Provider o Peering pubblici e privati;
7. Guasti e/o disservizi comunicati dal Cliente ma non riscontrati da WKI;
8. Indisponibilità del Servizio per aggiornamenti dei database degli enti ufficiali che gestiscono regole, infrastrutture e protocolli Internet (Ripe, Nic, ecc.)

I valori di SLA quivi illustrati potranno subire variazioni, nel corso della durata del Contratto, previa comunicazione scritta al Cliente con preavviso di 30 (trenta) giorni.