Wolters Kluwer Italia S.r.l.
Via Bisceglie, 66
20152 Milano (MI)
Tel. +39 02 824761
Fax +39 02 82476799

Allegato A | DOCUMENTO DI SLA
(Service Level Agreement)

Sommario

Wolters Kluwer Italia S.r.l.
Via Bisceglie, 66
20152 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, Cod. Fiscale e P.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.

Il cliente fornisce autorizzazione generale alla nomina di ulteriori sub-responsabili del trattamento a termini e condizioni conformi a quelle stabilite dal presente documento. Resta fermo che WKI avrà in tal caso l'obbligo di comunicare l'avvenuta nomina al cliente, fermo restando il diritto del cliente di opporsi alla modifica del sub-responsabile ed eventualmente di recedere dal contratto per giusta causa e senza responsabilità alcuna.

Il Cliente fornisce autorizzazione generale a che WKI nomini i seguenti soggetti sub responsabili del trattamento:

Nome: Microsoft Corporation Inc.
Indirizzo: 1950 N Stemmons Fwy Ste 5010 LB #842467 DALLAS TX 75207 United States.

Descrizione del trattamento: Servizio Microsoft Azure

Dati gestiti in Microsoft Azure nel territorio Europeo:
· Sito primario: Region West Europe (Amsterdam)
· Sito secondario: Region North Europe (Dublino)

Resta ferma inoltre la responsabilità solidale di WKI con i propri sub-responsabili nei confronti del cliente.

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:

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, così come è fatto divieto a WKI di accedere ai dati del cliente per finalità diverse da quelle relative all'erogazione del servizio, in conformità al regolamento GDPR.

4.2 Accesso al servizio SaaS

Il cliente può accedere 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 incidenti 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/explore/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

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.

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

Policy di backup dei dati.

In SuiteNext viene utilizzato il Point-In-Time Restore (PITR) presente in Azure SQL Database che permette di ripristinare il database in qualsiasi istante entro il periodo di retention (35 giorni).

Nell'ambito del PITR le frequenze con cui vengono effettati i backup (gestiti da Microsoft, conservati online) sono indicate nel seguito:

- Full Backups: settimanalmente.
- Differential Backups: ogni 12 ore.
- Transaction Log Backups: ogni 5-10 minuti.

Per ciascuna delle tipologie indicate sopra, la retention è la stessa del PITR e cioè 35 giorni.

Policy di backup dei documenti.

I documenti di SuiteNext sono conservati in opportuni container di istanze di Microsoft Azure BlobStorage. Tali istanze sono geo-replicate e pertanto una replica di ogni documento è presente in ciascuna regione di backup. Per tali istanze è abilitato il Point-In-Time Restore (PITR) che dà la possibilità di ripristinare una 'fotografia' dei container ad un qualsiasi istante entro il periodo di data retention (35 giorni).
A livello di container è inoltre abilitato il versioning dei documenti che permette di ritrovare anche precedenti versioni di un documento modificato.

È possibile avere maggiori info sull'ubicazione dei backup e dei dati del cliente a questo indirizzo:
https://learn.microsoft.com/en-us/azure/azure-sql/database/automated-backups-overview

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 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. 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).

6.1 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.

6.2 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 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.

6.3 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 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.

Wolters Kluwer Italia S.r.l.
Via Bisceglie, 66
20152 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, Cod. Fiscale e P.IVA 10209790152
R.E.A. di Milano N. 1353036

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)
Altri incident	Entro 2h → Lunedì ÷ Venerdì 09:00 ÷ 18:00 (festivi esclusi)

SLA di servizio (disponibilità infrastruttura)		
Availability	Business Hours 9/18 Mon/Fri	99,78%
	Operating Hours	
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%

6.4 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		

7. SLA sui servizi e moduli aggiuntivi | eSignAnyWhere

Ove il cliente acquisti il modulo eSignAnyWhere, sono indicati di seguito gli SLA sui servizi.

eSign AnyWhere (eSAW) è la piattaforma di firma Namirial, integrata in SuiteNext per la digitalizzazione delle transazioni di business e dei workflow documentali, con particolare riferimento alla fase di sottoscrizione. È sviluppata da Namirial S.P.A., una società IT di software e servizi nonché Certification Authority, che fornisce Trust Services come Firme Elettroniche, Grafometriche e Digitali, Posta Elettronica Certificata, Fatturazione Elettronica e Conservazione Sostitutiva.

eSAW garantisce un sistema di firma in grado di gestire transazioni complesse, fruite in multicanalità (e-mail, web, mobile, etc...) e da più utenti contemporanei (concorrenza). L'approccio impiegato per realizzare le componenti applicative della soluzione eSAW e cioè il front end ed i moduli che interagiscono direttamente con gli utenti, con le applicazioni e con i siti client, è quello di un web-service.

7.1 Tipologie di firme supportate

Con eSign Anywhere è possibile eseguire le seguenti tipologie di firma:

Firma Elettronica

- È possibile firmare i documenti utilizzando i meccanismi di Click to Sign, Type to Sign, Draw to Sign.
- Cliccando sul campo firma vengono apposte tutte le informazioni collegate al firmatario (nome, mail, indirizzo IP, timestamp).
- Nel caso Type to Sign, il destinatario firma inoltre digitando il proprio nome che viene reso in corsivo sul campo firma, mentre nel caso Draw to Sign: Il firmatario disegna la propria firma con un dito, una penna o il mouse.
- Per ogni firma viene utilizzato un certificato non qualificato riconosciuto da Adobe che garantisce l'integrità e immodificabilità del documento.

Firma Elettronica Avanzata (FEA)

- I meccanismi di cui sopra possono essere utilizzati per implementare una FEA, se viene rispettato quanto previsto in relazione al processo di adozione di una FEA previsto all'art.57 del DPCM 22 Febbraio 2013 (identificazione del firmatario, informativa sul processo, etc.).
- È possibile implementare una FEA, sia grazie all'utilizzo di un OTP SMS che permette di firmare con una Strong Authentication, che attraverso l'acquisizione dei dati biometrici rilevati durante l'apposizione della firma sui dispositivi supportati.

Firma Elettronica Qualificata (FEQ)

È possibile firmare un documento con FEQ utilizzando:

- un certificato digitale remoto rilasciato dal Certificatore Namirial. Per firmare basta inserire il nome utente di Firma Remota Namirial il PIN e la One Time Password;
- un certificato digitale di tipo Disposable. Per firmare basta inserire One Time Password;
- un certificato digitale su SmartCard / USB Token. Per firmare basta inserire il PIN.

La Firma Elettronica

Per Firma Elettronica s'intende un insieme di dati in forma elettronica, riconducibili all'autore, allegati oppure connessi ad atti o fatti giuridicamente rilevanti contenuti in un documento informatico, utilizzati come metodo di identificazione informatica.

La normativa riconosce alla firma elettronica un valore probatorio: la firma è liberamente valutabile dal giudice in fase di giudizio, in base a caratteristiche oggettive di qualità e sicurezza del sistema informatico e di integrità e immodificabilità del documento Informatico.

Al fine di garantire le caratteristiche di cui sopra, la piattaforma utilizza i seguenti metodi:

- Il documento da firmare viene inviato alla mail indicata dal firmatario cui egli ha accesso grazie a credenziali in suo possesso.
- Prima di accedere al documento da firmare può essere richiesto l'inserimento di una One Time Password (OTP) inviata via SMS al numero di cellulare indicato dal firmatario.
- Con ogni firma viene apposto sul documento un timbro in cui sono indicati il nome e cognome del firmatario, la sua mail, l'indirizzo IP dal quale ha effettuato la connessione e la data/ora UTC.
- L'integrità del documento viene garantita attraverso l'apposizione di una firma tecnica effettuata attraverso un certificato di firma non qualificato per ogni firma apposta.

Viene generato un Audit Trail o Log di tutti i passi effettuati con inclusi gli IP address e la eventuale geolocalizzazione del firmatario.

Date & Time	Action	Description	Signer	IP Address	Geolocation
2016-10-23 I 16:30:51	WorkstepCreated	SignAnyWhere workstep created			
2016-10-23 I 16:31:20	CalledPage	SignAnyWhere loaded using v5.6.58.19967		82.56.71.204	N/A
2016-10-23 I 16:31:21	WhoIsInformation	Organization: Telecom Italia S.p.A. TIN EASY LITE city: Paderno Dugnano country: Italy lat: 45.569 lon: 9.1648	Antonio Taurisano	82.56.71.204	N/A
2016-10-23 I 16:31:26	PrepareAuthenticationSuccess	Prepared authentication for provider 'Sms' Phone number: +393409510216 Transaction ID: hMgS0IPFgv Expiration time: 10/23/2016 14:36:25 UTC	Antonio Taurisano	82.56.71.204	45.61°/9.26° ±65m <city />
2016-10-23 I 16:33:59	AuthenticationSuccess	Authenticated with provider 'Sms' Phone number: +393409510216 Code: 5416 Transaction ID: hMgS0IPFgv Expiration time: 10/23/2016 15:33:59 UTC	Antonio Taurisano	82.56.71.204	45.61°/9.26° ±65m <city />
2016-10-23 I 16:34:03	PageViewChanged	Page 1 shown	Antonio Taurisano	82.56.71.204	45.61°/9.27° ±192.34285707298756m <city />
2016-10-23 I 16:34:13	Draw2SignDialogClosed	Signature dialog with id '1#XyzmoDuplicateIdSeperator#94a96f23-2234-65d5-af87-dbfa2cee62f5' was closed!	Antonio Taurisano	82.56.71.204	45.61°/9.26° ±65m <city />
2016-10-23 I 16:34:33	Draw2SignDialogClosed	Signature dialog with id '1#XyzmoDuplicateIdSeperator#94a96f23-2234-65d5-af87-dbfa2cee62f5' was closed!	Antonio Taurisano	82.56.71.204	45.61°/9.26° ±65m <city />
2016-10-23 I 16:35:01	SignWorkstepDocument	Document (SigField 1#XyzmoDuplicateIdSeperator#94a96f23-2234-65d5-af87-dbfa2cee62f5) has been signed on page 1 of document #1 by Antonio Taurisano using signature type 'Picture'	Antonio Taurisano	82.56.71.204	45.61°/9.26° ±65m <city />
2016-10-23 I 16:35:05	WorkstepFinished	Workstep has been finished	Antonio Taurisano	82.56.71.204	45.61°/9.26° ±65m <city />

7.2 Modalità di firma

Il sistema eSAW è in grado di implementare funzionalità di apposizione delle firme digitali e/o elettroniche secondo differenti modalità.

La modalità standard è quella interattiva in cui i firmatari accedono ad un Web Signature Tray (Viewer) all'interno del quale è possibile visualizzare e firmare i documenti proposti seguendo un wizard particolarmente intuitivo.

La modalità interattiva, prevede un flusso secondo il quale un'applicazione oppure un sito internet richiedono la firma digitale di un documento attraverso la creazione di una pratica (o transazione) di firma.

I documenti da firmare possono essere protetti da un meccanismo di autenticazione per assicurarsi che solamente il firmatario designato possa accedervi. I meccanismi di autenticazione disponibili sono:

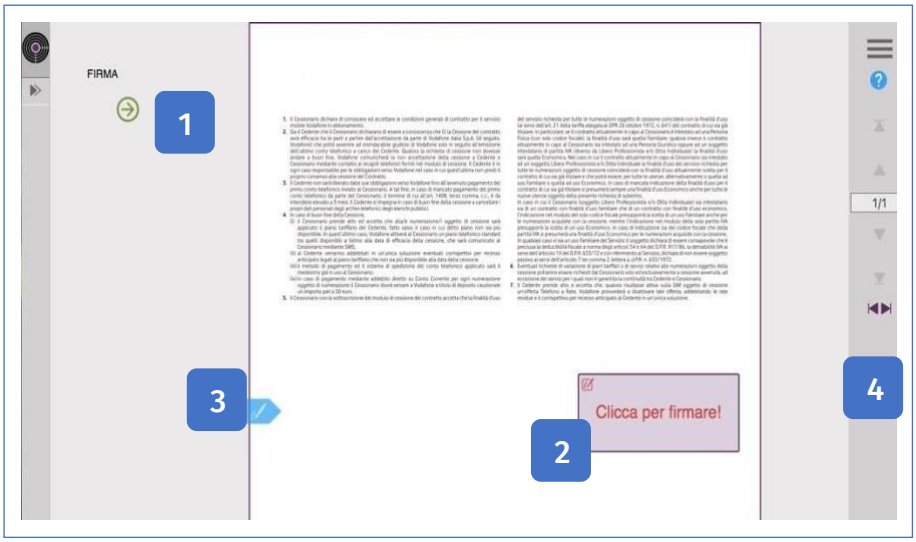
- Un PIN comunicato al firmatario designato "out-of-band";
- Un OTP inviato sul numero di cellulare del firmatario (dispositivo personale).

Il sistema eSAW crea la pratica di firma e genera una URL univoca che la identifica e può essere direttamente utilizzata nel browser del firmatario designato.

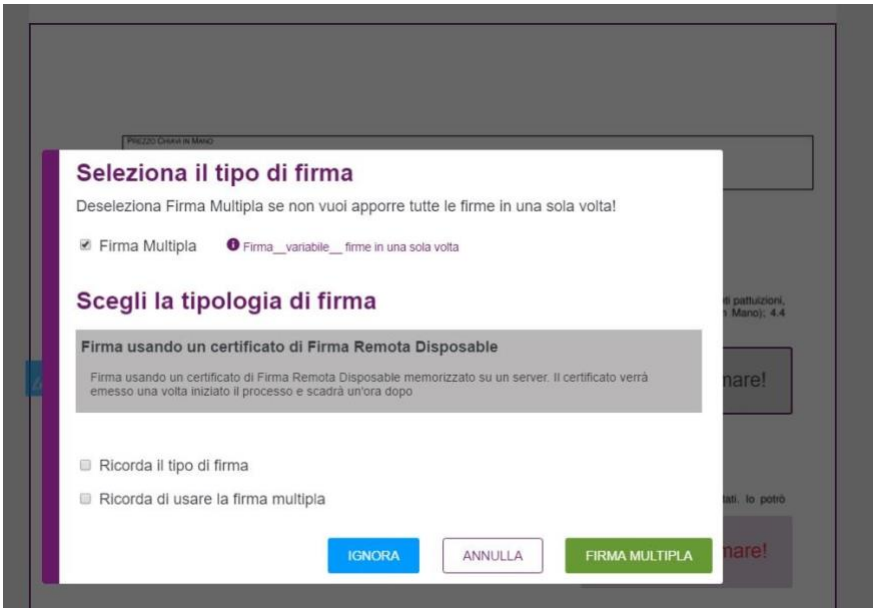
Accedendo con un browser alla URL della transazione di firma, viene mostrato il Viewer, ovvero un'interfaccia che presenta:

- Un'anteprima del documento da firmare.
- I controlli di firma.
- Il wizard di firma
- Menu con Guida e azioni accessorie per l'utente.

Alla pressione del tasto di firma l'utente viene invitato a scegliere la tecnologia di firma pre-impostata dal sistema per la particolare tipologia di documento a disposizione.

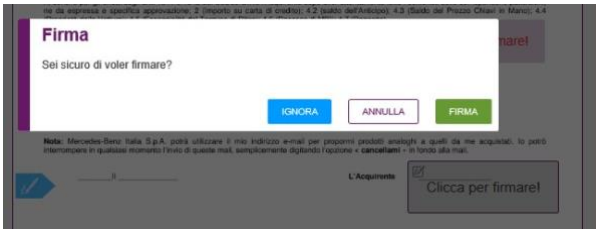


Di seguito è riportata un'immagine esplicativa del Viewer di eSAW.



eSAW, Selezione tipologia di firma

L'utente seleziona la tipologia di firma e procede con la sottoscrizione del documento.
Di seguito è riportata la user-experience nel caso di flusso di firma elettronica.



eSAW, Completamento firma elettronica semplice

Tramite eSignAnyWhere è possibile utilizzare anche la Firma Grafometrica (firma elettronica avanzata) tramite app o signature pad in grado di raccogliere dati biometrici.

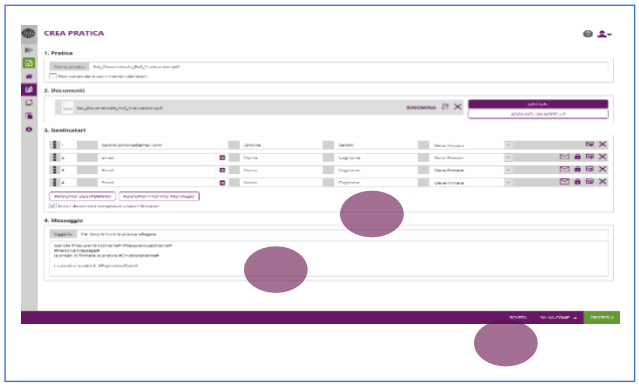
Wolters Kluwer Italia S.r.l.
Via Bisceglie, 66
20152 Milano (MI)
Tel. +39 02 824761
Fax +39 02 82476799

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

7.3 Progettazione della pratica

Una volta caricato il documento oggetto della transazione eSAW consente di impostare:

1) set e sequenza dei firmatari con la possibilità di definire sia firmatari in sequenza che in parallelo;
2) la possibilità di trasmettere i documenti a tutti firmatari o ad un gruppo ristretto;
3) la possibilità di mostrare un messaggio esplicativo che guidi il firmatario nello svolgimento dell'operazione di firma.



Le azioni da associare ad un destinatario possono essere:

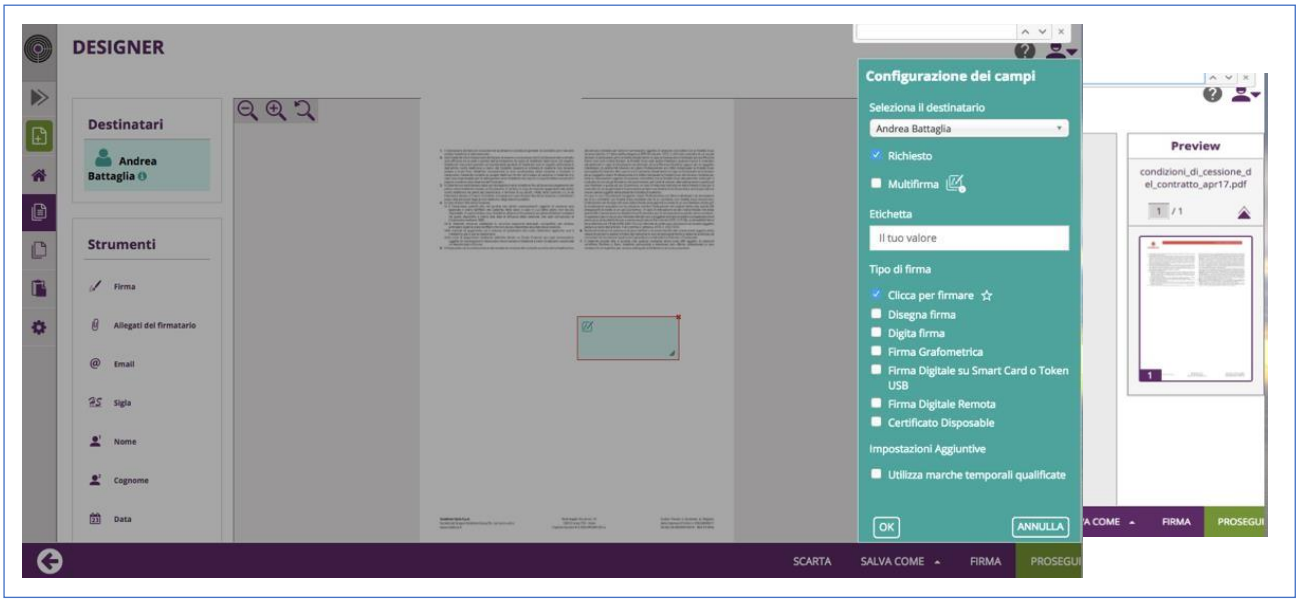
- Firma.
- Copia Conoscenza.
- Presa Visione.

Per ogni destinatario è possibile definire anche un meccanismo di autenticazione tramite PIN, OTP o Windows Live.

Completata la selezione dei firmatari e delle altre informazioni accessorie, eSAW permette all'applicazione invocante di configurare aspetto e tipologia di firme da inserire nel documento oltre ad un'altra serie di altri parametri che, nel complesso, concorrono al miglioramento della transazione e dell'esperienza utente.

In particolare, è possibile:

1) aggiungere campi firma, testo, allegati e altre informazioni accessorie al documento;
2) configurare la/e tipologia/e di firma/e con cui ciascun firmatario potrà sottoscrivere.



Una volta finalizzata la pratica eSAW ritorna un URL che può essere inviata per e-mail o consumata direttamente all'interno dell'applicazione invocante (es pagine web).

7.4 Orari e livelli del servizio

Il servizio è erogato e monitorato 24x7x365. Sulle piattaforme Namirial è garantito un up-time mensile del servizio applicativo del 99,5% con esclusione delle finestre di maintenance comunicate con un preavviso di almeno 24 ore.

7.5 Architettura tecnica-applicativa

Schema di deployment: Public cloud (shared SaaS). La piattaforma è gestita da Namirial.

7.6 Certificazioni di Namirial

Namirial S.p.A. è accreditata per l'emissione di certificati qualificati conformi al regolamento europeo 910/2014 e alla normativa nazionale in materia, Gestore di PEC, Gestore SPID e Conservatore presso AgID (ed DigitPA).

La società è inoltre certificata ISO 9001:2015 – ISO/IEC 27001:2013, certificata da Adobe e membro dell'AATL (adobe approved Trust List). Ha inoltre ottenuto la certificazione eIDAS e relative norme ETSI per l'emissione di validazioni temporali, certificati qualificati e sigilli elettronici nonché la certificazione Electronic Identity relativamente ai servizi Fiduciari di Identificazione Elettronica.

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

Il Cliente potrà usufruire dei Servizi di assistenza e di interventi in teleassistenza sul Programma applicativo e sui moduli aggiuntivi integrati 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.

I tempi di presa in carico delle richieste, a prescindere che siano state inoltrate via ticket o tramite e-mail, sono dettagliati nella tabella che segue:

		Urgenza			
TEMPO PER LA PRESA IN CARICO		1 – Impossibile eseguire operazioni fondamentali (accesso al programma, perdita di dati, ...)	2 – Errore del programma per il quale è presente un work-around, anche se complesso	3 – Problema minore per il quale è presente un work-around con basso impatto sull'operatività	4 - Richiesta di informazioni o problema minore che non ha impatto sull'uso del sistema
Priorità	1. Critica	4 ore	2 giorni	10 giorni	10 giorni
	2. Alta	1giorno	4 giorni	15 giorni	20 giorni
	3. Media		10 giorni	30 giorni	45 giorni
	4. Bassa		15 giorni	45 giorni	60 giorni

9. 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.

Formato dei dati

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 ".csv". Relativamente ai documenti, gli stessi saranno resi disponibili in uno storage on line, organizzati per cartelle (una cartella per ogni pratica individuata dal codice pratica) e nello stesso formato originale con cui sono stati trattati (es. docx, xlsx, etc.). I file saranno memorizzati esattamente con lo stesso nome memorizzato nel software gestionale. La consegna, senza spese aggiuntive a carico del Cliente, avverrà entro 30 giorni lavorativi dal giorno di cessazione del contratto.

Su richiesta del Cliente, i dati si possono ottenere in altro formato previe verifiche tecniche preliminari e con modalità, tempi e costi da concordare. Tutto ciò che non è espressamente riportato in questo articolo, 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.

10. 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.
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: I SP 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.

Luogo e data

Cliente (Timbro e Firma)

_____ _____