

Wolters Kluwer Italia S.r.l.
Via Bisceglie n. 66
20152 Milano
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, C.Fisc. e P.Iva 10209790152
R.E.A. di Milano N. 1353036

Kleos

Descrizione del trattamento dei dati personali e misure tecniche e organizzative



Descrizione del trattamento dei dati personali e delle misure tecniche e organizzative relative alle prestazioni

La presente Scheda viene emessa ai sensi del Contratto e dell'Addendum sul trattamento dei dati ("DPA") tra il Fornitore e il Cliente e ne costituisce parte integrante.

1. Trattamento dei dati personali

Il presente documento è emesso ai sensi, e costituisce parte integrante, del Contratto di nomina responsabile del trattamento dei dati ("DPA", Data Processing Agreement) tra il Fornitore e il Cliente.

Nell'esecuzione del Contratto, il Fornitore può trattare i Dati personali del Cliente, in qualità di Responsabile del trattamento, per conto del Cliente e in conformità con le istruzioni dello stesso, per fornire i Servizi software e/o i Servizi professionali inclusi, laddove applicabile, quelli per:

- Installazione e configurazione
- Hosting e monitoraggio in Kleos
- Migrazione dei dati
- Assistenza e manutenzione

1.1. Categorie di dati personali trattati

In qualità di Titolare del trattamento, il Cliente può inserire, memorizzare e trattare i suoi Dati, inclusi quelli personali, in Kleos. Il Fornitore, in qualità di Responsabile del trattamento, non è a conoscenza della natura dei Dati personali creati, inseriti e caricati dal Cliente prima della immissione in Kleos.

Nella sua configurazione standard, Kleos fornisce campi di base, compilabili dal Cliente per trattare i Dati personali, quali nome, indirizzo, numero di telefono, indirizzo e-mail, data di nascita, ecc.

È, inoltre, possibile inserire ulteriori informazioni facoltative, se necessarie per la gestione di determinati contesti aziendali (es. indirizzo aziendale, telefono aziendale, ecc.), in base allo scopo del Trattamento definito dal Cliente. La presenza di tali campi è il risultato di una scelta deliberata da parte del Cliente, ed è, pertanto, di esclusiva responsabilità del Cliente.

Ai fini dell'erogazione delle prestazioni di cui al Contratto, il Fornitore potrà trattare le seguenti categorie di Dati Personali:

A. Dati dell'utente

- Nome e Cognome
- Codice Fiscale
- Genere
- Password
- Funzione
- Facoltativo: recapiti (e-mail, telefono, indirizzo)

B. Dati dei clienti/parti del procedimento

- Nome e cognome e titolo, se specificato
- Codice Fiscale
- Recapiti (e-mail, telefono, indirizzo)
- Data di nascita
- Professione
- Stato civile
- Profilo azienda
- Dati finanziari
- Coordinate bancarie e modalità di pagamento
- Dati di fatturazione
- Dati fiscali
- Documenti inerenti al mandato conferito

I dati personali vengono immessi dagli Utenti tramite le funzioni del software per le finalità qui descritte. I dati personali dei clienti/parti non sono raccolti direttamente presso i soggetti interessati. I dati personali immessi in Kleos dal Titolare del trattamento sono a esclusiva discrezione e rischio dello stesso.

1.2. Categorie di soggetti interessati

In qualità di Titolare del trattamento, il Cliente può inserire, memorizzare e trattare in Kleos i dati personali dei seguenti soggetti:

- dipendenti, partner contrattuali e clienti;
- altri soggetti (quali, ad es., parti in causa, avvocati della controparte, periti, testimoni).

1.3. Finalità del trattamento

Il Cliente, in qualità di titolare del trattamento, è responsabile della determinazione delle finalità del trattamento effettuato con Kleos. Kleos può essere utilizzato per i seguenti scopi:

- gestione fascicoli ;
- adempimento del mandato;
- comunicazione con i clienti;
- parcellazione;
- dati a tribunali, compagnie assicurative, terzi, etc.

Per il corretto funzionamento di Kleos non è necessaria alcuna interconnessione con altri sistemi e, in particolare, nessuna informazione sarà esportata verso altri sistemi dall'elenco delle persone. Le interconnessioni stabilite tra Kleos e altri sistemi gestiti e/o richiesti dal Cliente sono sotto la supervisione e la responsabilità esclusiva del Cliente.

1.4. Natura del trattamento

Il trattamento dipende dai servizi forniti dal Responsabile dello stesso ai sensi del Contratto e può includere la registrazione, l'organizzazione, la modifica, l'estrazione, il recupero, la consultazione, la divulgazione tramite trasmissione, l'archiviazione, la limitazione, la cancellazione e la distruzione.

1.5. Periodo di conservazione

In qualità di Titolare del trattamento, il Cliente determina il periodo di conservazione dei Dati personali gestiti in Kleos (contratti, controversie, informazioni di contatto, documenti correlati, ecc.).

Il Fornitore memorizza i Dati del Cliente e ne esegue il backup nell'esecuzione del presente Contratto, in conformità con le disposizioni dello stesso, comprese quelle del presente Allegato.

Il Fornitore, in qualità di Responsabile del trattamento, conserva i Dati del Cliente, inclusi, laddove possibile, i Dati personali, nei seguenti casi e per i seguenti periodi di conservazione (fatti salvi gli obblighi di legge o i termini di prescrizione):

- dati personali gestiti tramite l'Assistenza (informazioni fornite dal Cliente per il supporto): i Dati del Cliente, compresi gli eventuali Dati personali, se presenti, saranno cancellati dai database di Assistenza del Fornitore sei (6) mesi dopo la scadenza del Contratto; in qualità di Titolare del trattamento, il Cliente si fa carico di minimizzare i dati personali trattati necessari alla gestione di segnalazione di errori da parte dei servizi di Assistenza del Fornitore;
- copia dei Dati del Cliente (DUMP) per il supporto: per risolvere un problema tecnico, il Fornitore potrebbe aver bisogno di ottenere o copiare parte dei Dati del Cliente, inclusi, se del caso, i Dati personali, in un ambiente di test dopo aver ottenuto il consenso del Cliente. Tali Dati verranno utilizzati al sol fine di risolvere il problema in questione e saranno eliminati dall'ambiente di test al massimo due (2) mesi dopo la gestione del problema;
- dopo la migrazione dei dati: il Fornitore conserverà i Dati migrati per un periodo di due (2) mesi al fine di eseguire le eventuali correzioni richieste. Il Cliente è responsabile della copia/backup dei dati e, se necessario, della loro messa a disposizione del Fornitore dopo questo periodo;
- dopo la risoluzione/scadenza del Contratto: nell'ambito dei servizi di reversibilità previsti dal Contratto, se presenti, i Dati del Cliente saranno trasmessi al Cliente nel formato prestabiliti. Il Fornitore conserverà, quindi, sui propri server i database pertinenti per trenta (30) giorni (o per un altro periodo specificato nel Contratto), prima della completa distruzione, fatti salvi gli obblighi di conservazione previsti dalla legge.

2. Misure di sicurezza tecniche e organizzative

Il Fornitore adotterà le misure di sicurezza tecniche e organizzative ("TOM", Technical and Organizational Measures) appropriate, valutate sulla base dello stato dell'arte al momento della sottoscrizione del Contratto, ed il Fornitore valuterà tali TOM nel tempo, tenendo conto dei costi di implementazione, della natura, dell'ambito, del contesto e delle finalità del Trattamento, nonché della probabilità di rischi per i diritti e le libertà degli interessati.

2.1. Controllo degli accessi: Datacenter / Hosting Infrastruttura IT

Ubicazione Datacenter	All'interno dell'UE/SEE (Spazio Economico Europeo) Datacenter primario: Germania, Francoforte Datacenter secondario: Germania, Berlino https://azure.microsoft.com/it-it/explore/global-infrastructure/geographies/#choose-your-region
Certificazione Datacenter	ISO/IEC 27001:2013
Ridondanza geografica	I dati dei clienti sono salvaguardati dalla perdita attraverso l'archiviazione con ridondanza geografica. Vedere Disaster Recovery.
Firewall applicazione web	All'interno dell'UE/SEE Servizi con instradamento del traffico limitato all'interno dell'UE https://www.cloudflare.com/it-it/data-localization

2.2. Protezione e recupero dei dati

Conservazione dei backup	Frequenza	Periodo di conservazione
	Giornaliero	30 giorni
	Settimanale (backup completo)	7 settimane
	Mensile (backup completo)	4 mesi
Backup esterni (su richiesta del cliente)	Il cliente ha la possibilità di richiedere un backup dei propri dati su richiesta e a pagamento. La fornitura del backup avviene online.	

2.3. Crittografia e protezione dello scambio di dati

Comunicazione client server	Protocollo HTTPS, protetto con TLS (Transport Layer Security) con versione 1.2 e AES 256.
Informazioni amministrative/metadati	Tutti i dati memorizzati vengono crittografati con AES256. Le chiavi di crittografia utilizzate per la cifratura sono archiviate e protette all'interno di un sistema di gestione delle chiavi sicuro, con un controllo degli accessi rigoroso, regolamentato dal Fornitore.
Dati memorizzati	Tutti i dati memorizzati vengono crittografati con AES256. Le chiavi di crittografia utilizzate per la cifratura sono archiviate e protette all'interno di un sistema di gestione delle chiavi sicuro, con un controllo degli accessi rigoroso, regolamentato dal Fornitore.
Dati in transito	La comunicazione con i client è protetta con crittografia TLS 1.2 e AES 256.
Gestione delle chiavi	Tutte le chiavi di crittografia sono protette attraverso l'utilizzo di un modulo di sicurezza hardware (HSM, Hardware Security Module).

2.4. Mezzi per garantire la riservatezza, l'integrità, la disponibilità e la resilienza continua dei sistemi e dei servizi di trattamento

Minimizzazione dei dati	Creazione di utenti La creazione di utenti richiede solo il cognome, il nome, il ruolo (profilo), l'indirizzo e-mail e la password dell'utente.
Limitazione del periodo di conservazione	Dati utente Anonimizzazione dei dati al momento della disattivazione dell'accesso degli utenti dal Cliente.
Informazioni sui dati	Le informazioni relative alla finalità del trattamento possono essere fornite in qualsiasi momento dagli utenti autorizzati.
Cancellazione dei dati	Operazioni di cancellazione manuale o anonimizzazione.
Rettifica dei dati	Gli indirizzi delle persone fisiche possono essere modificati in qualsiasi momento dagli utenti autorizzati.

2.5. Procedure per testare, accertare e valutare periodicamente l'efficacia delle misure tecniche e organizzative volte a garantire la sicurezza del trattamento

Scansioni di sicurezza	La soluzione tecnica Kleos viene regolarmente controllata per verificare la presenza di vulnerabilità di sicurezza.
Penetration Test	Il prodotto Kleos viene periodicamente testato da penetration tester interni ed esterni.
Business Continuity Plan (BCP)	Il piano di continuità operativa (BCP) per la piattaforma Kleos comprende una strategia dettagliata e una serie di sistemi per prevenire interruzioni significative delle operazioni o per eseguire un ripristino rapido, se necessario. Il Fornitore ha sviluppato un piano di continuità operativa per la piattaforma Kleos e lo revisiona a intervalli regolari.
Livello dell'infrastruttura	Kleos viene scansionato periodicamente.
Funzioni di archiviazione Kleos (ad es. caricamento di documenti)	Quando un file viene trasferito nel prodotto Kleos (ad esempio, il salvataggio di un documento), viene verificata la presenza di contenuti dannosi.
Raccomandazioni	Il Cliente dovrà implementare un'adeguata sicurezza sui propri dispositivi. Si consiglia al Cliente di proteggere tutti i dispositivi dall'accesso non autorizzato, attraverso password o controlli di sicurezza biometrica. Allo stesso modo, si consiglia di installare e aggiornare su tutti i dispositivi software di crittografia dati e sistemi antivirus. Il Cliente dovrà assicurarsi che il sistema operativo venga aggiornato regolarmente.

3. Report sugli incident

Per il tracciamento degli incidenti utilizziamo il tool sviluppato internamente "Elsatrace". La base giuridica per questo trattamento è costituita dall'art. 6, comma 1, lett. b) del GDPR.

Quali dati vengono raccolti da Elsatrace?

I dati raccolti comprendono: l'identificativo dell'utente e del database, la descrizione, il codice e l'ora esatta dell'errore.

Come utilizza Wolters Kluwer le informazioni raccolte?

Le informazioni raccolte vengono utilizzate per fornire ai nostri sviluppatori dettagli sulle funzionalità e sulle eventuali anomalie riscontrate.

Esiste un modo per gli utenti per impedire la raccolta di dati e informazioni?

No.

Utilizziamo lo strumento ETL (Extract, Transform, Load) sviluppato internamente da Wolters Kluwer per analizzare l'utilizzo e raccogliere i seguenti dati:

Dati di utilizzo

- Nome del database
- Richiesta di connessione
- Tempo impiegato dalla richiesta
- Frequenza di utilizzo delle funzioni e delle relative opzioni.

I dati trasmessi sono esclusivamente quelli sopra indicati. In particolare, non vengono trasmessi dati personali dei singoli utenti (ad es. nome, località, chiave di registrazione, indirizzo IP del cliente). In nessun caso i dati trasmessi al Fornitore sono cedibili ai singoli utenti.

I dati di cui sopra vengono trasmessi automaticamente. La trasmissione avviene solitamente ad ogni sessione, alla chiusura dell'applicazione. Tutti i dati trasmessi sono crittografati e inviati tramite https. Prima della trasmissione, i dati vengono memorizzati in forma non crittografata sul disco rigido del PC del singolo utente. In questo modo ogni utente ha la possibilità di accertarsi che non vengano trasmessi dati personali.

Finalità e base giuridica del trattamento dei dati

Gli strumenti analitici vengono utilizzati, tra le altre cose, per migliorare la facilità d'uso, l'efficacia e la sicurezza dei nostri prodotti. A tale scopo, il Fornitore necessita di informazioni sull'hardware e sul software dello studio legale e sulle modalità di utilizzo degli utenti.

Periodo di conservazione

I dati relativi alle segnalazioni di incidenti non vengono conservati in modo permanente. I dati di utilizzo vengono conservati per 12 mesi.

Possibilità di opporsi

L'utente non ha la possibilità di disattivare questa trasmissione di dati.

4. Sub-appaltatori

Le società affiliate identificate nell'accordo di trasferimento infragruppo in vigore all'interno di Wolters Kluwer sono le seguenti:

Nome	Indirizzo	Attività	Localizzazione dei dati
Wolters Kluwer Technology B.V.	Zuidpoolsingel 2 2408 ZE Alphen aan den Rijn Paesi Bassi	Sviluppo software e supporto di secondo livello	Paesi Bassi
Wolters Kluwer Italia S.r.l.	Via Bisceglie 66, 20152 Milano	Assistenza di secondo livello	Residenza dati: Germania
Wolters Kluwer Global Business Services Italia	Via Bisceglie 66, 20152 Milano	Gestione del cloud	<p>Microsoft Azure <u>Datacenter primario:</u> Germania Ovest - Francoforte sul Meno</p> <p><u>Centro dati secondario:</u> Germania Nord - Berlino</p> <p>Web Application Firewall (WAF): Microsoft Azure Deutschland Servizi regionali Cloudflare gestione limitata del traffico all'interno dell'UE</p> <p><u>Residenza dei dati:</u> Germania Wolters Kluwer Technology B.V. Zuidpoolsingel 2 2408 ZE Alphen aan den Rijn, Olanda, Softwareentwicklung und 2nd-Level-Support, Olanda</p>
Wolters Kluwer Global Business Services Italia	Via Bisceglie 66, 20152 Milano	Gestione dei server del portale di start-up e formazione clienti	Microsoft Corporation Inc Region: West Europe, Amsterdam, Microsoft's campus on the Agriport A7

Terzi subappaltatori

Nome	Indirizzo	Attività	Localizzazione dei dati
T-Systems International GmbH	Centro dati di Monaco/Allach Dauchauer Strasse 665 80995 München Centro dati di Monaco/Eip Elisabeth Selbert Strasse 1 80939 München	Hosting di Kleos	Germania
Salesforce.com	Piano 26 Salesforce Tower, 110 Bishopsgate, EC2N 4AY Londra Regno Unito	Gestione dei ticket di supporto	Regno Unito
Namirial SpA	Z.I Predda Niedda Nord strada, 5 07100 Sassari	Fatturazione elettronica	Italia
Net Service Spa	Via Marche, 8/10, 27010 Siziano (PV)	Gestione Punto di Accesso (PdA) al processo Civile Telematico	Italia
Legos S.r.l.	Via F.lli Rosati, 33 Gioia del Colle (BA)	Servizi di configurazione tecnica iniziale, formazione iniziale e assistenza di primo livello	
Net Service Spa	GoTo Technologies Ireland Unlimited Company 77 Sir John Rogerson's Quay, Block C, Suite 207, Grand Canal Docklands Dublin 2, Ireland	Supporto remoto	