DocuSign e la sua conformità legale

- Oltre 300.000 clienti paganti e oltre 200 milioni di utenti in tutto il mondo.
- Sette delle prime 10 aziende tecnologiche globali.
- Diciotto tra le prime 20 aziende farmaceutiche globali.
- Dieci delle prime 15 società di servizi finanziari globali.

Più di 300.000 aziende e organizzazioni di tutto il mondo si “af-fidano” a DocuSign per firme elettroniche giuridicamente vincolanti, con circa 2.000.000 documenti firmati tutti i giorni. Le policy di sicurezza world-class adottate da DocuSign e una user experience intuitiva rende la raccolta di firme elettroniche giuridicamente vincolanti facile e conveniente.

Come soddisfa DocuSign i requisiti di legge?

DocuSign è stato sviluppato per soddisfare i requisiti legali delle firme elettroniche nel mondo a partire dal ESIGN Act e altre leggi USA, consentendo agli utenti di:

- verificare l’identità del firmatario con molteplici forme di autenticazione;
- confermare l’intento del firmatario di firmare elettronicamente;
- collegare le firme ai firmatari e ai documenti (autenticità e integrità);
- registrare tutte le principali attività legate alla vita del documento e alla firma;
- permettere, in qualsiasi momento, l'accesso sicuro ai documenti DocuSign;
- proteggere i documenti con sistemi/sigilli anti contraffazione, che utilizzano una combinazione di processi di protezione del sistema e la tecnologia PKI (Public Key Infrastructure).

DocuSign fornisce la prova per le firme elettroniche giuridicamente vincolanti

Per ogni documento, DocuSign genera automaticamente e memorizza, marcandola temporalmente, la storia completa di ogni invio, visualizzazione, stampa, firma, o azione di rigetto/rifiuto. Questa informazione viene catturata nel Certificato di Completamento DocuSign che viene generato per ogni transazione DocuSign. Qualsiasi parte coinvolta nella transazione, che vuole rivedere l'attività associata ad un documento, è in grado di visualizzare, scaricare o stampare il Certificato di Completamento associato al documento.

Con oltre 250 milioni di transazioni firmate, le firme elettroniche DocuSign non sono mai state ripudiate, o contestate con successo in qualsivoglia tribunale nel mondo. Nel caso di una controversia legale connessa ad una firma elettronica, la società DocuSign supporta direttamente i propri clienti.

DocuSign utilizza processi sicuri

DocuSign offre il sistema leader del settore per la sicurezza del processo, per salvaguardare i documenti, le firme e i dati. Questo fornisce garanzie legali aggiuntive per le autenticazioni e gli audit trail creati durante una transazione.

DocuSign è l'unico fornitore di firma elettronica ad essere certificato ISO 27001 sui sistemi interni, sulla ingegneria di processo, e sulle operazioni di business. È certificato, o compatibile con le certificazioni di sicurezza più stringenti del settore per la firma elettronica, l'archiviazione dei dati, la riservatezza dei dati e la sicurezza dei pagamenti.

- DocuSign fornisce il più alto livello di garanzia di sicurezza essendo l'unica società di gestione delle transazioni digitali al mondo ad essere certificata sia ISO 27001:2013 che xDTM, così come SSAE 16, SOC 1 Type 2, SOC 2 Type 2.
- DocuSign garantisce la riservatezza dei dati con livello di crittografia AES 256 bit.
- I controlli anti-manomissione garantiscono l'integrità dei documenti dei clienti, sia in fase di processo che una volta completati.
- Tempi pressoché in real-time, replica di dati sicura e uptime del 99,99%.
- DocuSign offre caratteristiche uniche per il non ripudio, tra cui audit digitale e catena di custodia.
- Terza parte indipendente nel processo di firma che vede coinvolti un proponente e un firmatario.

Opzioni avanzate per la conformità e la riduzione del rischio

DocuSign offre la più ampia scelta di opzioni di autenticazione avanzate incorporate per verificare l'identità del firmatario. L'utilizzo dell'autenticazione forte o più livelli di autenticazione riducono/eliminano il rischio di ripudio. DocuSign offre molteplici livelli di autenticazione che consentono a un mittente di determinare con accuratezza come un firmatario si deve identificare, compreso l'uso di e-mail, social network ID, codici di accesso, SMS, telefono, e controlli d'identità basati su basi di conoscenza.

Le opzioni di firma elettronica avanzata offerte da DocuSign, la maggior parte basate sulla tecnologia della firma digitale PKI, riducono il rischio per transazioni regolamentate ad alto valore, nel pieno rispetto delle norme locali, come eIDAS (regolamento UE 910) e ICP Brasil.

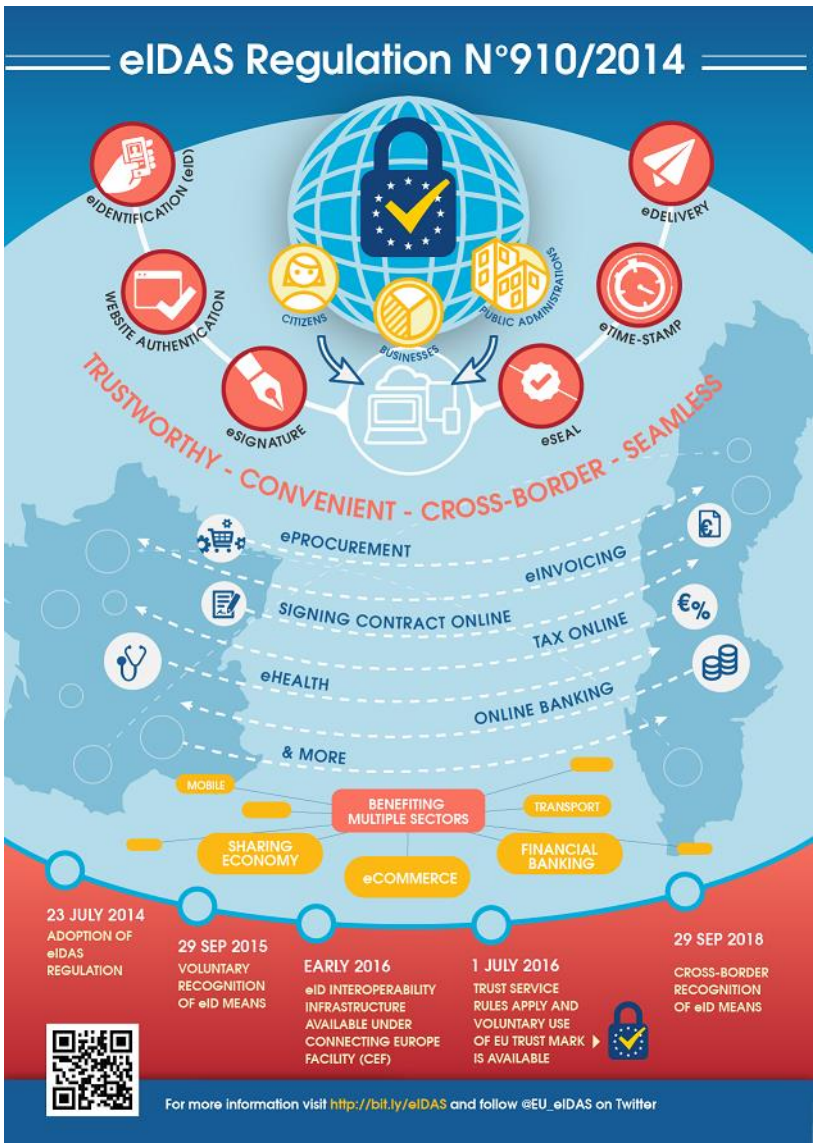
Nella UE, DocuSign offre tutti i tipi di firma definiti nel regolamento eIDAS, comprese le firme elettroniche qualificate e le firme elettroniche avanzate, insieme alla presenza di tre data center nell'Unione Europea.

GDPR compliance

Essendo un'organizzazione focalizzata sulla fiducia dei clienti e sulla gestione dei loro documenti, DocuSign ha sviluppato una forte cultura della conformità e solide garanzie di sicurezza, che si riflettono nella

sua certificazione ISO 27001 e nelle sue Binding Corporate Rules (BCR) approvate. Gli sforzi di conformità GDPR di DocuSign fanno leva su queste risorse. DocuSign sta attivamente monitorando gli orientamenti del regolatore e le interpretazioni dei principali requisiti GDPR per allineare i propri sforzi e, come molti fornitori di servizi cloud, sta attualmente rivedendo la propria policy di protezione dei dati, apportando modifiche per garantire il rispetto del Regolamento generale sulla protezione dei dati (GDPR) entro il 25 maggio 2018.

Il contesto di riferimento europeo



Il Regolamento (UE) n 910/2014 sui servizi di identificazione e di fiducia elettronici per le transazioni elettroniche nel mercato interno (meglio conosciuto come il regolamento eIDAS) ha trovato applicazione diretta in tutti gli Stati membri dell'Unione europea dal 1 ° luglio 2016, quando è entrato in vigore in maniera completa e la precedente direttiva sulla firma elettronica del 1999 è stata abrogata. Il nuovo quadro

giuridico garantisce la certezza giuridica per l'uso transfrontaliero di firme elettroniche, sigilli elettronici, marche temporali, servizio di eDelivery e certificati di autenticazione di siti Web.

Le principali modifiche introdotte dal regolamento eIDAS sono:

- un regolamento, non una direttiva, che le rende direttamente applicabili in tutta Europa senza che sia necessario il recepimento nella legislazione nazionale;
- aprono la strada a nuove soluzioni di firma qualificate remote e a una migliore esperienza utente;
- un'armonizzazione paneuropea della firma elettronica;
- ai documenti elettronici non è possibile negare l'effetto giuridico solo perché sono in formato elettronico;
- servizi fiduciari qualificati in tutta Europa
- l'introduzione di sigilli elettronici, disponibili per le persone giuridiche, tecnologicamente simili alla firma elettronica e che garantiscono identità e integrità;
- la costituzione delle Trusted List nazionali mutuamente riconosciute fra stati membri;
- un servizio di validazione qualificato per firme elettroniche qualificate.

Nel Regolamento eIDAS n° 910/2014 non esiste una singola firma elettronica. Le firme elettroniche sono divise in tre, a seconda della tecnologia utilizzata e del livello di sicurezza e privacy offerto all'utente. In particolare, il regolamento europeo parla di:

1) semplice firma elettronica (ad es. Email personale);
2) firma elettronica avanzata (ad esempio firma grafometrica su un dispositivo mobile);
3) firma elettronica qualificata (fornita da un QTSP UE – Qualified Trust Service Provider).

Articolo 25

Effetti giuridici delle firme elettroniche

1. *A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate.*

2. *Una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa.*

3. *Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri.*

Nel regolamento eIDAS sia le firme elettroniche qualificate che non qualificate (semplici e avanzate) beneficiano di una clausola di non discriminazione come prova nei tribunali. In altre parole, un documento firmato digitalmente non può essere scartato dal giudice solo sulla base del fatto che sia in formato elettronico.

Nello specifico la firma elettronica avanzata garantisce:

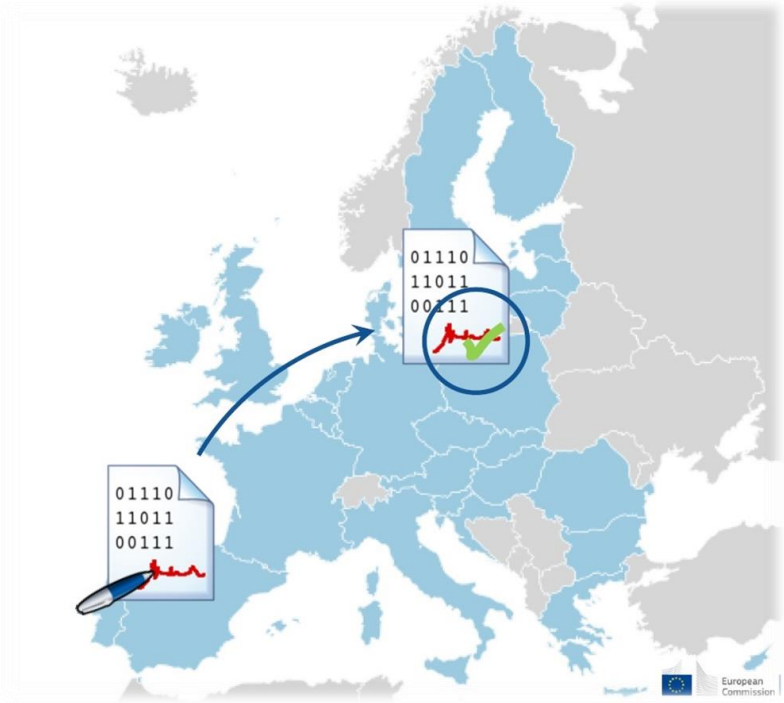
- l'identificazione del firmatario del documento;
- la connessione univoca della firma e del documento al firmatario;
- il controllo esclusivo del firmatario del sistema di generazione della firma (inclusi gli eventuali dati biometrici);
- l'integrità del documento firmato.

Tuttavia, a causa dei requisiti più severi applicabili ai prestatori di servizi fiduciari qualificati (QTSP), le firme elettroniche qualificate forniscono un effetto giuridico specifico più forte rispetto a quelle non qualificate e una maggiore sicurezza tecnica. I servizi fiduciari qualificati forniscono quindi maggiore certezza del diritto e maggiore sicurezza delle firme elettroniche.

Sebbene diversi livelli di firma elettronica possono essere appropriati in diversi contesti,

	Strengths	Weakness	Opportunities	Threats
Qualificata	Alto valore legale (inversione dell'onere della prova)	Diffusione più costosa	Conformità normativa semplice da verificare	No
Avanzata	Meno costosa	Valore legale medio (la prova spetta a chi fornisce lo strumento)	Facilita la realizzazione di processi B2C	Una implementazione debole espone a rischi
Grafometrica	Intuitiva e (in teoria) più semplice da usare	Valore legale medio. Formati proprietari . Strumenti di verifica non standard	Facilita la realizzazione di processi B2C	Una implementazione debole espone a rischi

solo le firme elettroniche qualificate sono esplicitamente riconosciute per avere l'effetto legale equivalente delle firme scritte a mano in tutta l'Unione Europea.



In definitiva …

DocuSign garantendo all'interno del suo processo DTM (Digital Transaction Management):

- l'identificazione del firmatario del documento;
- la connessione univoca della firma e del documento al firmatario;
- il controllo esclusivo del firmatario del sistema di generazione della firma;
- l'integrità del documento firmato
- la selezione del livello di valore legale della firma digitale (qualificata/erga omnes ed avanzata/inter partes)

si configura come soluzione DTM dal pieno valore legale.