CONDIZIONI GENERALI DI SERVIZIO ("CGS")

PER L'UTILIZZO DELLA FIRMA ELETTRONICA AVANZATA ("FEA")

Art. 1 – Informazioni preliminari e definizioni

Per quanto non espressamente disciplinato dalle presenti CGS, si rinvia – anche ai fini definitori – a quanto stabilito dalle disposizioni di cui agli atti di seguito richiamati:

1) Codice dell'Amministrazione Digitale (D.Lgs. 07 marzo 2005 n. 82 e successive modificazioni; di qui in avanti, "**CAD**");

2) Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali di cui al DPCM 22 marzo 2013 ("**Regole Tecniche**");

3) Regolamento UE 910/2014 ("**eIDAS**").

Il servizio di FEA è offerto da Victor Insurance Italia S.r.l. (sede legale in Via Calabria, n. 31 - 20158 Milano; di seguito, "**Victor**"), in qualità di soggetto che eroga soluzioni di firma elettronica avanzata (ai sensi e per gli effetti di cui all'art. 55, c. 2, lett. a) delle Regole Tecniche), avvalendosi delle soluzioni realizzate da un soggetto terzo.

Ai sensi e per gli effetti di cui all'art. 55 comma 2 lett. b) delle Regole Tecniche, il servizio di FEA è realizzato da DocuSign Inc. (221 Main Street, Suite 1000, San Francisco, CA 94105), in qualità di soggetto che realizza in proprio soluzioni di FEA a favore di altri soggetti, affinché questi le utilizzino nei rapporti intrattenuti con i propri clienti.

Il servizio offerto da Victor ai propri clienti (di seguito, "**Cliente**", "**Soggetto Sottoscrittore**", "**Sottoscrittore**") consiste nell'erogazione della FEA, ovvero di una soluzione di firma elettronica che consente ai Clienti di sottoscrivere validamente documenti che avranno la stessa efficacia giuridica e probatoria riconosciuta dal nostro ordinamento alle scritture private (art. 2702 del Codice Civile).

Art. 2 – Termini e condizioni del servizio

Ai fini della validità della FEA, l'ordinamento richiede la verifica dell'identità del Soggetto Sottoscrittore. L'identificazione del Soggetto Sottoscrittore richiede:

i) la consegna di un valido documento di riconoscimento da parte del Sottoscrittore secondo quanto specificato all'art. 3 che segue.

Art. 3 – Attivazione e utilizzo del servizio

Il Cliente attiva il servizio di FEA accedendo (mediante *click* sul tasto "Rivedi Documenti") al *link* trasmesso a mezzo e-mail all'indirizzo di posta elettronica comunicato dal Cliente via e-mail a Victor anche per il tramite dei propri collaboratori

Il *link* condurrà ad una pagina web, all'interno della quale verrà richiesto al Cliente di compilare un modulo di identificazione per verificare la sua identità. Si richiede di inserire le informazioni riguardanti l'ID: dove viene rilasciato (il paese) ed il tipo di ID (passaporto o ID con foto). Dopodiché, è necessario caricare il documento tramite cellulare o caricando il file

(entrambi i lati) seguendo le indicazioni sul sito. Una volta concluso il processo di identificazione, il Cliente potrà procedere con la sottoscrizione del documento.

Per procedere è necessario accettare le CGS cliccando sul campo *Visualizza* e poi sul campo *Accetta*. Una volta accettato, il Cliente può procedere con la firma del documento cliccando sul campo *Firma.*

Per finalizzare il processo della FEA, il Cliente deve controllare i suoi dati ed accettare i termini del Contratto dell'abbonato della firma avanzata EU *(selezionando Firma, si accetta di firmare il documento/documenti contenuti nella busta identificata dall'ID 'XYZ', confermando che il nome e l'indirizzo email del firmatario sono corretti ed accettando i termini del Contratto dell'abbonato della firma avanzata EU)*.

Art. 4 – Revoca del servizio

Il Cliente potrà revocare il consenso al momento della firma. Se il firmatario decide di revocare il proprio consenso deve selezionare '*rifiuta*', dopodiché verrà visualizzata una casella per inserire il motivo del rifiuto del documento. Il testo verrà inviato a Victor e verrà registrato come parte della cronologia della busta.

La revoca del consenso al servizio comporta l'impossibilità da parte del Cliente di accedere ed utilizzare il servizio di sottoscrizione di documenti tramite FEA.

Art. 5 – Ambito di utilizzo

Il cliente potrà utilizzare la firma elettronica avanzata esclusivamente nei rapporti intercorrenti tra Victor ed il cliente stesso. Inoltre, il servizio di FEA, nelle attuali implementazioni, consente al Cliente di sottoscrivere contratti/documenti che riguardano anche i contratti, per cui è prevista la FEA, che egli intende stipulare con le società di cui Victor colloca/distribuisce prodotti.

Art. 6 - Conservazione del documento informatico sottoscritto. Conservazione di ulteriore documentazione

DocuSign provvede all'archiviazione digitale dei documenti sottoscritti dal cliente con firma elettronica avanzata. DocuSign provvede inoltre all'archiviazione della dichiarazione di accettazione delle presenti CGS e del documento di riconoscimento trasmesso dal Cliente per un periodo di almeno 20 anni, in ottemperanza a quanto prescritto dalle previsioni normative. Il Cliente potrà chiedere copia del documento di riconoscimento e dell'ulteriore documentazione di cui al paragrafo precedente inviando apposita richiesta all'indirizzo . cdp@pec.victorinsurance.it

Art. 7 - Copertura assicurativa

In conformità a quanto previsto nel DPCM 22 febbraio 2017 (art. 57, comma 2) è stata stipulata una polizza assicurativa per la responsabilità civile da danni derivanti dalla fornitura del servizio di firma elettronica avanzata e cagionati da soluzioni tecniche inadeguate.

CARATTERISTICHE TECNICHE

DocuSign è la piattaforma che Victor ha scelto per il servizio di firma elettronica dei documenti. Identificato come il Provider più affidabile e più utilizzato a livello mondiale, grazie a DocuSign è possibile accedere in qualsiasi momento ai documenti firmati, inviandoli senza correre il rischio di perderli. DocuSign è un servizio di facile utilizzo che permette la riservatezza dei dati che vengono crittografati in maniera sicura, inoltre la versatilità e l'aderenza alle normative rendono il processo di firma elettronica legalmente accettato in tutto il mondo.

DocuSign implementa un modello di firma elettronica avanzata con l'ID verifica (la verifica del documento di riconoscimento del firmatario) gestito all'interno del servizio che viene richiesto prima della firma poiché consente di autenticare il firmatario in modo sicuro. DocuSign supporta la firma elettronica avanzata (remota) nei seguenti modi:

Identificazione univoca del firmatario

DocuSign consente di utilizzare la verifica dell'ID per verificare automaticamente l'identità dei firmatari e fornire firme elettroniche avanzate ai sensi del Regolamento UE n. 910/2014 (c.d. Regolamento eIDAS). Grazie alla verifica dell'ID DocuSign è in grado di associare in maniera univoca il firmatario alla firma elettronica.

Cosa viene verificato sull'ID? DocuSign verificherà che:

- L'ID non è scaduto
- Il nome corrisponde alla busta come specificato dal mittente
- Le MRZ ('*machine readable zones*'), come il codice a barre, vengono decodificate in informazioni coerenti con il resto dell'ID
- Le caratteristiche visive / ologrammi sono coerenti con l'aspetto che dovrebbe avere quel tipo di ID
- Non ci sono prove di manomissioni dei caratteri, spaziatura delle lettere, buchi o altri difetti nell'ID
- Non vengono effettuate chiamate ai database governativi, poiché molti richiedono privilegi dedicati

Se un ID non viene riconosciuto automaticamente, il firmatario non sarà in grado di accedere ai documenti. Il team specificato che gestisce la FEA riceve una notifica di annullamento busta per mancata identificazione e provvedere a verificare i dati attraverso la piattaforma Il team contatta il cliente tempestivamente per le istruzioni del caso e provvede ad inoltrare nuovamente il documento, così che i firmatari possano accedere nuovamente e provvedere alla nuova verifica.

Crittografando come BLOB (Binary Large Object), il sistema DocuSign protegge l'integrità dei documenti (inclusa la verifica dell'ID) e dei tag mentre i dati sono at rest. Oltre alla crittografia BLOB, protegge i dati in transito abilitando le connessioni TLS all'interno delle API eSignature e delle applicazioni web. In più, ha implementato i certificati SSL (Secure Socket Layer) emessi da DigiCert (un'autorità di certificazione considerata attendibile dai

sistemi operativi / browser web). DocuSign fornisce la crittografia end-to-end che copre sia i dati at rest che i dati in transito. Inoltre, utilizza l'hashing dei dati SHA-2 per il controllo dell'integrità all'interno del nostro sistema.

DocuSign garantisce la connessione univoca della firma e consente un controllo esclusivo del firmatario del sistema di generazione della firma. DocuSign, infatti, fornisce sessioni di firma uniche per tutti i firmatari. I firmatari vengono identificati in modo univoco tramite e-mail, e la verifica dell'identità. Delle informazioni sopra menzionate ne viene conservata traccia, il Certificato di completamento.

Attraverso DocuSign i firmatari hanno la possibilità di scaricare una copia dei documenti firmati in qualsiasi momento durante/dopo la sessione di firma. A tutti i firmatari è inoltre consegnata una copia finale dei contratti attraverso la posta elettronica. Le copie dei documenti firmati possono essere ottenute in formato pdf o attraverso un collegamento ipertestuale.

Inoltre, DocuSign garantisce la connessione univoca della firma del documento sottoscritto. Attraverso DocuSign il completano dei requisiti da parte dei firmatari avviene al momento della sessione di firma. Tutte le sessioni sono uniche e crittografate in transito e "*at rest*". Una volta che una busta (transazione) è stata completata, l'accordo finalizzato è inserito digitalmente in un sistema digitale a prova di manomissione.

Archiviazione di documenti

DocuSign provvede all'archiviazione della dichiarazione di accettazione delle presenti CGS e del documento di riconoscimento trasmesso dal firmatario per un periodo di almeno 20 anni, in ottemperanza a quanto prescritto dalle previsioni normative. Tutti i dati vengono archiviati nei data center dell'UE. I dati possono essere recuperati tramite *API ID Evidence Rest*, che utilizza la crittografia TLS (*Transport Layer Security*) affidabile e il protocollo HTTPS sulla porta 443.

Inserimento di un sigillo nel documento firmato (per rilevare eventuali modifiche ai dati)

Una volta apposta la firma elettronica sui documenti, DocuSign inserisce nei documenti un sigillo di antimanomissione (attraverso il metodo "hash" e la crittografia) utilizzando un certificato digitale globale di firma.

Procedure consigliate in caso di controversie

In caso di controversie riguardanti un contratto stipulato per via elettronica, DocuSign garantisce la raccolta e la conservazione di molti elementi che possono risultare determinanti in caso di controversia per impedire eventuali disconoscimenti di una firma. Di seguito l'elenco completo degli elementi disponibili a tale scopo:

1) Itinerario di controllo con contrassegno di ora/data di tutte le azioni svolte dal firmatario.

2) Crittografia protetta che consente di leggere e firmare i documenti solo agli utenti designati.

3) Firme univoche create da ciascun utente, accessibili solo dagli utenti corrispondenti (team specifico che gestisce la FEA in Marsh) e memorizzate online in maniera protetta.

4) Aree di firma (Stick-eTab) richieste, che consentono ai firmatari di apporre le iniziali e la firma su parti specifiche del documento.

Intenzione di apporre la firma

Nei documenti cartacei la collocazione precisa della firma è un criterio importante per stabilire l'intenzione del firmatario. DocuSign consente tale trasposizione anche nella forma elettronica.

Elementi di protezione della firma

I documenti firmati tramite la piattaforma DocuSign hanno una protezione completa in quanto viene tenuta traccia delle persone che hanno firmato, del tipo di autenticazione con i suoi dati, dell'ora e della data in cui le firme sono state apposte. Tale processo di controllo è definito "certificato di completamento": il certificato di completamento e i documenti firmati in maniera digitale con sigillo di garanzia sono gli elementi chiave per eseguire un corretto processo di FEA.

Ammissibilità in sede probatoria

Gli Stati membri dell'Unione Europea, tra cui anche l'Italia, prevedono l'ammissibilità in sede probatoria dei record elettronici e delle riproduzioni di questi ultimi.

Nel caso della Firma Elettronica Avanzata, l'Art.21 del D.lgs n.85/2005 e ss.mm.ii. -Codice dell'Amministrazione Digitale (CAD) stabilisce che, in caso di disconoscimento, con l'adozione di tale metodologia di firma, risulti fondamentale dimostrare ai tribunali quanto segue:

1) L'identificazione del firmatario e la connessione univoca dello stesso al documento firmato;

2) Tale connessione è creata utilizzando dei mezzi sui quali il firmatario può conservare il controllo esclusivo;

3) La possibilità di rilevare se i dati sono stati modificati successivamente all'apposizione della firma elettronica avanzata.

Il documento informatico sottoscritto con firma elettronica avanzata che garantisca i requisiti di cui sopra, ha l'efficacia prevista dall'articolo 2702 del codice civile, il quale stabilisce che: *"La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta".*

Datacenter

La piattaforma DocuSign eroga il servizio in modalità Software as a Service (SaaS) in regime di Business Continuity attraverso i datacenter ridondati localizzati in Parigi (Francia), Amsterdam (Olanda) e Francoforte (Germania). I dati trattati all'interno del servizio offerto sono dunque memorizzati esclusivamente all'interno del territorio dell'Unione Europea. Tutti i datacenter sono oggetto di certificazione ISO 27001, 27017, 27018, PCI DSS e SSAE 18.