Condizioni generali di DeepCloud SA per l'utilizzo di DeepID (gennaio 2024)

1. In generale

1.1 Il presente documento contiene le condizioni generali (**CG**) di DeepCloud SA, Abacus-Platz 1, 9300 Wittenbach, Svizzera (**DeepCloud**) per l'utilizzo del servizio DeepID e della relativa app DeepID (**DeepID**).

1.2 DeepID consente di accertare l'identità di una persona fisica (**identificazione**), di invitare altre persone a identificarsi (affinché possano verificare un'organizzazione in qualità di persone con diritto di firma), di autorizzare determinate manifestazioni di volontà (come il rilascio di determinate firme elettroniche) o atti, nonché di **autenticare e autentificare** nell'ambito di determinate applicazioni di DeepCloud o di fornitori terzi. Per le prestazioni utilizzate da un fornitore terzo con l'ausilio di DeepID, viene stipulato un contratto esclusivamente tra l'utente di DeepID (**utente**) e il rispettivo fornitore terzo.

1.3 Con le presenti CG, DeepCloud disciplina diritti e doveri, nonché altri aspetti determinanti in relazione all'utilizzo di DeepID.

1.4 Il consenso dell'utente a queste CG avviene nell'ambito del processo di identificazione nell'app DeepID. L'utente dichiara in tal modo di essere il legittimo detentore del mezzo di autenticazione (per esempio smartphone, tablet) e di avere il controllo esclusivo di tale mezzo di autenticazione, nonché di essere a conoscenza dei diritti e degli obblighi di cui alle CG, di acconsentirvi e di attenersi alle CG. L'utente garantisce di essere maggiorenne e di poter esercitare i diritti civili necessari a consentirgli di impegnarsi al rispetto delle presenti CG. I minori di età compresa tra i 16 e i 18 anni provvedono a ottenere il consenso necessario dei detentori dell'autorità parentale.

2. Prestazioni di DeepCloud

2.1 Con DeepID, DeepCloud mette a disposizione dell'utente un servizio di identificazione, verifica, autorizzazione e autenticazione per diversi campi di applicazione.

2.2 A tal fine, DeepCloud propone l'app DeepID. Tale applicazione può essere scaricata dai relativi app store.

3. Identificazione dell'utente tramite l'app DeepID

3.1 Prima del primo utilizzo delle funzionalità di DeepID occorre confermare l'identità dell'utente. A tal fine, l'utente segue i passaggi previsti nell'app DeepID. Indica la propria nazionalità e il proprio domicilio ed esibisce un documento d'identità valido. L'utente conferma la proprietà e il controllo esclusivo del proprio dispositivo inserendo nell'app DeepID il codice a quattro cifre inviatogli via e-mail. Durante la procedura, l'utente definisce il PIN del proprio dispositivo e può anche utilizzare la protezione di accesso del proprio dispositivo (come la biometria del dispositivo (impronte digitali/riconoscimento facciale) o il codice PIN) per l'accesso a DeepID.

3.2 Una volta confermata l'identità dell'utente tramite un documento d'identità valido e una volta effettuati i controlli, l'utente può utilizzare la sua DeepID tramite l'app. Essa viene salvata come tale con tutti i ruoli e gli attributi (con ID e dati di accesso).

3.3 Al momento della registrazione e del trattamento dei dati dell'utente nell'ambito della procedura di identificazione, dall'utente vengono acquisiti e confrontati anche i dati biometrici estratti dalle foto e dai video realizzati, nonché dal suo documento d'identità. Solo così è possibile provare l'identità in modo affidabile. Con la presente, l'utente acconsente espressamente al trattamento dei propri dati biometrici ai fini dell'accertamento della propria identità.

3.4 Lo svolgimento dettagliato della procedura di identificazione e quali dati siano stati raccolti e trattati in tale contesto sono descritti nell'informativa sulla protezione dei dati di DeepCloud, nella sezione «Trattamento dei dati in caso di utilizzo delle nostre applicazioni mobili (app)» alla voce «Servizio DeepID e app mobile DeepID (Android e iOS)». DeepCloud ha il diritto di adeguare e modificare per motivi legittimi le procedure di accertamento dell'identità. L'utente dovrebbe pertanto consultare regolarmente l'informativa sulla protezione dei dati di DeepCloud per conoscerne eventuali modifiche.

3.5 Qualora l'utente desideri utilizzare la propria identità DeepID confermata per servizi di fornitori terzi, possono sussistere, a seconda del servizio, determinate limitazioni o condizioni dovute a condizioni di utilizzo diverse. Tali limitazioni o condizioni devono essere rispettate.

3.6 Nell'ambito della procedura di identificazione, l'utente deve comunicare determinati dati e realizzare foto e video di se stesso e del proprio documento d'identità. Le foto e i video devono essere obbligatoriamente realizzati dall'utente stesso.

3.7 L'utente deve verificare che tutti i dati da lui registrati ed indicati siano scevri da errori di lettura o di trascrizione, o ripetere su richiesta passaggi non conclusi correttamente (come la realizzazione di foto e video), altrimenti la procedura non può essere portata a termine. Egli è tenuto a fornire dati completi, corretti e aggiornati sulla propria persona. In particolare, devono essere confermati e, se necessario, corretti i dettagli relativi alla sua identità, come rilevabili dal documento d'identità e dalle sue indicazioni.

3.8 È necessario che il dispositivo dell'utente sia registrato come mezzo di autenticazione per l'utilizzo di DeepID conformemente ai requisiti prestabiliti. L'utente conferma in tal modo di essere il legittimo detentore del mezzo di autenticazione (per esempio smartphone, tablet) e di avere il controllo esclusivo su di esso.

3.9 Per aumentare la sicurezza dell'app DeepID, l'utente deve attenersi alle norme di sicurezza richieste (come l'attivazione della protezione d'accesso). A tal fine, egli crea un PIN a 6 cifre, attiva la protezione d'accesso al dispositivo (come Face ID, impronta digitale), nonché il blocco automatico dello schermo per sbloccare l'app DeepID. Inoltre, DeepCloud gli fornisce un codice di ripristinoche deve essere conservato in modo sicuro. In determinati casi, sarà possibile ripristinare l'accesso a DeepID solo tramite tale codice. Esiste la possibilità di generare un nuovo codice di ripristino.

3.10 L'identificazione dell'utente richiede l'adempimento di determinati requisiti che devono essere verificati e confermati (come carta d'identità, foto, video). Se i requisiti sono soddisfatti, il controllo viene effettuato in modo completamente automatico, altrimenti solo durante i normali orari di ufficio di DeepCloud. L'utente deve organizzarsi di conseguenza se desidera, per esempio, rilasciare tempestivamente delle firme elettroniche tramite DeepID. DeepCloud impiega a tal fine persone appositamente formate per svolgere le procedure di identificazione. All'occorrenza, possono essere necessari ulteriori accertamenti. In tal caso, l'utente ne verrà informato tramite il supporto (per esempio all'interno dell'app DeepID o per e-mail).

3.11 Una volta confermata la propria identità, l'utente può utilizzare le funzionalità di DeepID, scegliere nelle impostazioni tra vari setting (quali, adeguamento dei dati del profilo, regolazione della sicurezza del dispositivo, modifica del PIN, aggiornamento del documento d'identità) o eseguire il logout da DeepID.

3.12 Dopo il logout, o in caso di tre tentativi di inserimento del PIN errati, l'utente deve seguire i passaggi previsti dall'app DeepID per potervi accedere nuovamente.

3.13 In determinati casi è necessaria una nuova identificazione (**re-identificazione**) dell'utente, come in caso di modifiche del documento d'identità utilizzato (p. es. foto, nome, sesso, nazionalità, scadenza del periodo di validità del documento d'identità, perdita del documento d'identità, modifiche del codice NFC), scadenza del periodo di validità dell'identità accertata per le firme elettroniche, cambio di dispositivo quale mezzo di autenticazione per DeepID (p. es. in caso di furto, perdita, sostituzione), nonché alla scadenza del periodo di validità dell'identità DeepID e in qualsiasi circostanza rilevante ai fini dell'accertamento dell'identità dell'utente. A tal fine, l'utente sceglie la funzione «Ho già una DeepID» o «Rinnova documento» e segue la procedura di identificazione prestabilita.

3.14 DeepCloud è autorizzata in qualsiasi momento ad interrompere o sospendere (a lungo termine) una procedura di identificazione con l'utente (p. es. in caso di discrepanze nelle informazioni, impossibilità di eseguirne l'identificazione) o a dichiarare nulla un'identità confermata con DeepID per motivi legittimi. Ciò non determina, per l'utente, l'insorgere di pretese (quali risarcimento danni) né di altri diritti.

4. Funzionalità dell'app DeepID

4.1 Nell'app DeepID sono visibili tutte le funzionalità per l'utente, tra cui «Scansiona codice QR», «Cronologia», «Organizzazioni», «Rinnova documento» o «Firme». DeepCloud è autorizzata in qualsiasi momento a modificare o ad annullare funzionalità esistenti, nonché ad aggiungerne di nuove.

4.2 L'ambito di utilizzo di DeepID consiste nella cessione dell'utilizzo su internet del software necessario a tale scopo, ai sensi dei diritti di utilizzo qui concessi, compresa la memorizzazione di dati. L'identità DeepID confermata può essere utilizzata sia direttamente tramite l'app DeepID che per altre applicazioni di DeepCloud, nonché tramite l'integrazione di applicazioni, software o app, anche di fornitori terzi.

4.3 La **funzionalità «Scansiona codice QR»** consente all'utente di eseguire la scansione di un codice QR e di svolgere l'azione in esso contenuta. Ciò può includere l'autorizzazione (come il rilascio di un'espressione di intenti o di un'azione) o l'autenticazione per un servizio DeepCloud o di terze parti (come il login, la conferma dell'identità o l'accesso al sistema).

4.4 La **funzionalità «Cronologia firme»** elenca le azioni effettuate mediante DeepID, come il rilascio di una firma elettronica.

4.5 La **funzionalità «Organizzazioni»** consente all'utente identificato di invitare altre persone, affinché eseguano anch'esse la procedura di identificazione tramite DeepID. Lo scopo degli inviti è quello di far identificare persone con diritto di firma per un'organizzazione, in modo tale che quest'ultima possa essere verificata. A tal fine, l'utente deve aprire un account DeepCloud presso DeepCloud. In esso può invitare persone che in seguito eseguiranno autonomamente la procedura di identificazione di DeepID, nell'ambito della quale le informazioni fornite verranno confrontate con fonti pubbliche.

4.6 Con la **funzionalità «Rinnova il documente»** l'utente è tenuto a eseguire autonomamente e tempestivamente una re-identificazione in caso di modifiche rilevanti. Gli viene così ricordato di eseguire una re-identificazione al momento della scadenza del periodo di validità del suo documento d'identità utilizzato per l'identificazione o di un certificato per la sua firma elettronica. L'utente deve perciò eseguire nuovamente la procedura di identificazione. L'utente accetta di ricevere tale promemoria nell'app DeepID e per e-mail.

4.7 La **funzionalità «Attività»** consente all'utente di autorizzare firme elettroniche avanzate e qualificate messe a sua disposizione da un fornitore di servizi di certificazione o fiduciari.

5. Possibilità di impiego dell'identità DeepID

5.1 L'identità confermata mediante DeepID può essere utilizzata per diverse applicazioni e, unitamente al mezzo di autenticazione, per autorizzazioni e autenticazioni.

5.2 Una richiesta di utilizzo viene effettuata tramite un servizio DeepService o da un fornitore terzo al di fuori dell'app DeepID (come l'invito a rilasciare una firma elettronica); occorre, in tal caso, accettare le rispettive disposizioni del fornitore terzo o di DeepCloud per tale servizio e attenervisi.

5.3 Qualora in occasione di una richiesta non sussista ancora un'identificazione valida, l'utente viene invitato a identificarsi. Nel caso in cui sussista già un'identificazione valida, ma il dispositivo utilizzato sia nuovo o i documenti d'identità debbano essere rinnovati (dopo un massimo di 5 anni o dopo la scadenza della loro validità, a seconda di quale dei due eventi si verifichi per primo), è necessaria una re-identificazione o il rinnovo dei documenti.

5.4 L'azione concretamente richiesta dipende dal rispettivo servizio e dalla possibilità di impiego selezionata. DeepID serve esclusivamente a consentire l'altro servizio. Per le prestazioni di cui l'utente fruisce presso un fornitore terzo utilizzando l'identità DeepID (p. es. come mezzo di identificazione in caso di iscrizione a un accesso sicuro o per il rilascio di una firma elettronica) viene stipulato un contratto tra l'utente e il rispettivo fornitore terzo. Dalle disposizioni contrattuali di tali fornitori terzi si possono evincere limitazioni all'utilizzo di DeepID per i loro servizi.

5.5 Presupposto per l'utilizzo del servizio del fornitore terzo è che l'utente si sia identificato con successo tramite l'app DeepID, che l'identità DeepID venga accettata da tale fornitore terzo e sia collegata in DeepID, e che l'utente autorizzi la relativa richiesta.

5.6 L'app DeepID trasferisce i contenuti raccolti nell'ambito della procedura di identificazione a DeepCloud o ai responsabili del trattamento coinvolti nell'identificazione e, in caso di richiesta, i contenuti all'uopo necessari a un fornitore terzo autorizzato ai fini dell'autenticazione dell'utente e dell'esecuzione della rispettiva azione richiesta. In tale contesto può aver luogo uno scambio di informazioni con o tra sistemi di un fornitore terzo o è possibile che dei contenuti vengano sincronizzati con i sistemi in questione. A tal fine, le parti coinvolte sono espressamente autorizzate ad eseguire gli accessi necessari, lo scambio tra i rispettivi sistemi e l'elaborazione dei contenuti. In tale contesto possono essere trasmessi e trattati dati personali, documenti e dati relativi alle operazioni. Con la presente, l'utente vi acconsente espressamente.

5.7 Il processo di autorizzazione o autenticazione di un servizio è il seguente: L'utente riceve dal rispettivo servizio una richiesta (per e-mail, tramite notifica push, SMS, ecc.) per dare l'autorizzazione nell'app DeepID sul proprio mezzo di autenticazione. Viene concesso a tal fine un determinato lasso di tempo, che può variare a seconda del servizio. Dopo l'accesso all'app DeepID, l'utente può rilasciare l'autorizzazione richiesta, come per esempio, una firma elettronica o un'altra azione (p. es. accesso ad applicazioni o login, trasmissione di dati). Non appena l'utente rilascia l'autorizzazione, tale informazione viene firmata digitalmente con una chiave crittografica memorizzata sul mezzo di autenticazione e il relativo fornitore di servizi riceve, mediante trasmissione cifrata, la conferma che l'autorizzazione è stata inviata dal dispositivo autorizzato (il fornitore di servizi può verificare l'informazione firmata con la chiave crittografica pubblica). Si può quindi presumere che l'autorizzazione sia stata concessa dalla persona giusta, e l'azione richiesta può essere concessa.

5.8 Se l'utente non ha rilasciato l'autorizzazione o non l'ha concessa in tempo utile, il fornitore di servizi riceve l'informazione che il nulla osta non è stato concesso e che manca l'autorizzazione o che l'autenticazione non ha avuto successo. DeepID consente l'autorizzazione o l'autenticazione dell'utente unicamente per servizi di fornitori terzi che accettano l'identità DeepID. Se l'utente non autorizza l'azione richiesta o non la autorizza tempestivamente, risponde egli stesso delle conseguenze che ne derivano.

5.9 L'app DeepID supporta l'autenticazione multi-fattore. Grazie a tale autenticazione, il dispositivo desiderato è legittimato come fattore supplementare mediante la procedura di identificazione e può essere impiegato per confermare l'azione richiesta. L'autenticazione a due fattori è una procedura di sicurezza nell'ambito della quale l'utente fornisce due caratteristiche distinte per legittimarsi o rilasciare un'esplicita manifestazione di volontà. Nel caso di DeepID, è il possesso del mezzo di autenticazione e, nel caso di autorizzazione o autenticazione, è l'app DeepID a fungere da secondo componente per confermare l'azione.

5.10 Nell'ambito della procedura di identificazione, il dispositivo utilizzato è autenticato mediante l'impiego della suite di autenticazione basata sull'intelligenza artificiale e incentrata sull'utente e può quindi essere utilizzato per autorizzazioni e autenticazioni per comunicare con fornitori terzi.

6. Possibilità di impiego dell'identità DeepID per firme elettroniche

6.1 L'identità DeepID può essere utilizzata per l'autorizzazione e l'autenticazione di firme elettroniche avanzate e qualificate. I fornitori di servizi di certificazione o fiduciari riconosciuti (fornitori) possono rilasciare a una persona identificata certificati avanzati per firme elettroniche avanzate (FEA) e certificati qualificati per firme elettroniche qualificate (FEQ) con marca temporale qualificata (servizi di certificazione o fiduciari). L'utente deve identificarsi solo una volta per poter firmare più volte, salvo i casi in cui è necessario eseguire una re-identificazione.

6.2 L'app DeepID consente di eseguire la verifica dell'identità di tale persona (**firmatario**) all'uopo necessaria. I servizi di certificazione o fiduciari in questione sono erogati da tali fornitori ai sensi della Legge federale svizzera sulla firma elettronica (**FiEle**) o del Regolamento UE in materia d'identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (**regolamento eIDAS**).

6.3 DeepCloud è il servizio di registrazione per FEQ e FEA incaricato da tali fornitori. Essa è soggetta al DeepCloud Trust Service Practice Statement (TSPS) di volta in volta in vigore. La sua conformità al TSPS è stata valutata e confermata da un organismo di certificazione riconosciuto (organismo di valutazione della conformità (OVC)) in Svizzera e nell'UE. DeepCloud è stato certificato secondo il seguente schema di valutazione della conformità (Norm of Accreditation System): ISO 17021-1:2015 (per ZertES) e ISO 17065-1:2013 (per eIDAS VO) per «Remote Identification Certification» secondo i requisiti di ZertES, VZertES, TAV (SR 943.032.1), EU eIDAS VO, ETSI TS 119 461, ETSI EN 319 401 e ETSI EN 419 241-1.

6.4 DeepCloud verifica l'identità del firmatario nell'ambito di una procedura di identificazione certificata con DeepID, senza che il firmatario in questione debba essere presente. In tale contesto, l'utente deve attenersi scrupolosamente alle prescrizioni e fornire sempre informazioni complete, corrette e aggiornate. Nel corso della procedura di identificazione, l'utente può essere invitato a esibire documenti diversi a seconda del motivo per cui l'identificazione deve essere utilizzata.

6.5 Qualora un'identificazione non possa essere eseguita con successo, DeepCloud ha il diritto di escludere un nuovo tentativo di identificazione nel breve o lungo termine. Se l'identificazione soddisfa tutte le condizioni necessarie, l'identità DeepID viene registrata ai fini della creazione di FEA e FEQ. Tale registrazione viene riesaminata prima di ogni incarico del firmatario.

6.6 In particolare, quando l'emissione di FEA o FEQ viene commissionata, sussistono condizioni speciali da soddisfare prima della loro autorizzazione da parte del firmatario. Il firmatario deve, infatti, essere domiciliato in Svizzera, nell'UE o nel SEE e deve confermarlo in occasione del conferimento dell'incarico di creazione di FEA e FEQ. In caso contrario, l'utente non può usufruire di tali servizi. Risponde pienamente delle possibili conseguenze derivanti dal mancato rispetto di tali requisiti. DeepCloud e i rispettivi fornitori terzi declinano in tal caso qualsiasi garanzia e responsabilità riguardo ai propri servizi.

6.7 Per l'identificazione ai fini dell'incarico di una FEQ e FEA sono ammessi esclusivamente i documenti di identità consentiti dai fornitori di servizi di certificazione o fiduciari a tal fine. Tali documenti si evincono dalla procedura di identificazione. I documenti di identità devono essere validi al momento dell'identificazione. L'elenco dei documenti di identità ammessi può variare, rendendo eventualmente necessaria una re-identificazione. Ai fini dell'identificazione e in caso di incarico da parte del firmatario possono essere utilizzati soltanto i documenti di identità prestabiliti dai fornitori di servizi di certificazione o fiduciari. Essi stabiliscono, inoltre, se il firmatario debba sottoporsi a una procedura di identificazione per ogni firma elettronica (firma singola) o se dopo la procedura di identificazione possa creare più firme elettroniche per un determinato periodo di tempo. Può eventualmente derivarne la necessità di una re-identificazione del firmatario.

6.8 Il firmatario viene invitato a rilasciare una firma elettronica tramite un servizio (come DeepSign, il servizio di firma di DeepCloud). A seconda del tipo di firma scelto, viene rilasciata una firma elettronica semplice (FES) oppure una FEQ o FEA conformemente alle disposizioni legali applicabili (FiEle o regolamento eIDAS). Non è ammesso utilizzarle in maniera diversa da quella per cui sono state rilasciate in occasione dell'incarico per i servizi di certificazione o fiduciari offerti da tali fornitori (limitazione d'uso).

6.9 DeepCloud registra e memorizza i dati relativi all'utente raccolti nell'ambito della procedura di identificazione DeepID e i contenuti necessari nella procedura di autorizzazione per i servizi di certificazione o fiduciari, secondo le disposizioni contrattuali e le norme vigenti.

6.10 I fornitori sono responsabili dell'emissione dei certificati e della coppia di chiavi crittografiche per la procedura di firma dopo il rilascio dell'autorizzazione da parte dell'utente. Il firmatario può utilizzare tale certificato unitamente ai propri dati di attivazione servendosi di DeepID. Non appena il firmatario, previo relativo incarico (accettando le condizioni di utilizzo del rispettivo fornitore e confermando il domicilio richiesto), abbia rilasciato la propria autorizzazione in DeepID, il rispettivo fornitore crea per lui la FEA o la FEQ sulla base di tale certificato. Per ogni procedura di firma viene creato un nuovo certificato digitale (con breve periodo di validità) con una nuova coppia di chiavi.

6.11 Con l'identificazione confermata tramite DeepID, l'utente può utilizzare il rispettivo servizio di certificazione o fiduciario per il periodo di validità dell'identificazione per tutte le applicazioni di firma che DeepCloud e i fornitori hanno collegato a DeepID per far creare una FEQ o FEA valida, senza che sia necessaria una nuova identificazione e fintantoché ciò sia ammesso dalla rispettiva applicazione di firma e dal periodo di validità del certificato.

6.12 DeepCloud verificherà l'identità del firmatario, lo autenticherà e gli consentirà di autorizzare.

6.13 I fornitori sono autorizzati a verificare presso DeepCloud, tramite audit, il rispetto dei propri obblighi contrattuali nell'ambito dell'identificazione, autorizzazione e autenticazione per FEA e FEQ. In tale contesto possono essere consultati anche dati del firmatario. I fornitori in questione possono far eseguire tale operazione dai propri collaboratori o da terzi e condividere i risultati con gli organismi di valutazione della conformità e le autorità di vigilanza competenti.

7. Diritti di utilizzazione, diritti di proprietà immateriale

7.1 DeepCloud concede all'utente un diritto d'uso personale, non esclusivo, non trasferibile, non cedibile, semplice, limitato nello spazio e nel tempo sul software impiegato per DeepID, per la durata del rapporto d'uso ad uso proprio e sul proprio mezzo di autenticazione. Ciò significa che solo l'utente può utilizzare DeepID per se stesso. La portata del diritto d'uso si evince dalle presenti CG.

7.2 È vietato all'utente rendere DeepID accessibile a terzi o metterlo loro a disposizione. L'utente non è inoltre autorizzato a destinare i software impiegati ad un utilizzo che si discosta da quello qui concesso da DeepCloud.

7.3 DeepCloud ha il diritto di offrire interfacce e di concedere licenze ad esse relative per l'esportazione di dati da DeepID in altri sistemi esterni, dove potrebbero essere ulteriormente trattati. L'utente può utilizzare tali interfacce con servizi, anche di fornitori terzi, solo nell'ambito del presente rapporto d'uso. Ciò vale anche nel caso in cui vengano impiegate interfacce allo scopo di utilizzare i dati tramite un altro sistema. L'utente deve attenersi alle possibilità di utilizzo e rispettare i limiti preimpostati da DeepCloud e non è autorizzato a eluderli servendosi di percorsi tecnici alternativi.

7.4 Il software utilizzato da DeepCloud può essere soggetto a prescrizioni in materia di controllo delle esportazioni e ad altre leggi. In tal caso, non può essere esportato, riesportato o trasferito in determinati Paesi o a persone o soggetti a cui è vietato ricevere determinate merci di esportazione (incluse quelle elencate nelle pertinenti liste di sanzioni per persone o soggetti). L'utente deve attenersi a eventuali prescrizioni locali relative all'utilizzo di servizi con tecnica di cifratura come quella utilizzata per DeepID.

7.5 Per quanto riguarda i software di fornitori terzi impiegati, si applicano le loro disposizioni di licenza.

7.6 L'utente è tenuto a informare immediatamente DeepCloud qualora terzi facciano valere nei suoi confronti diritti di proprietà intellettuale (p.es. diritti d'autore o diritti dei brevetti) relativi al software durante l'utilizzo di DeepID. L'utente non intraprende alcuna azione legale senza l'autorizzazione di DeepCloud e non può accettare, di propria iniziativa, alcuna pretesa da parte di terzi senza il consenso di DeepCloud. DeepCloud adotta a proprie spese tutte le misure di patrocinio necessarie, come la difesa contro pretese di terzi, nella misura in cui non si fondino sul comportamento illecito dell'utente.

7.7 L'utente prende atto del fatto che il proprio app store non è tenuto in alcun modo a fornire servizi di manutenzione e di supporto relativi all'app DeepID. Se un terzo rivendica il fatto che DeepID o il possesso dell'app DeepID violi i propri diritti di proprietà intellettuale, è DeepCloud e non l'app store a rispondere della difesa contro tali pretese.

7.8 Tutti i diritti di proprietà intellettuale su DeepID (incluso il software all'uopo impiegato), su contenuti, testi, immagini, fotografie, video, loghi o altre informazioni di DeepCloud, compresi i relativi siti web, appartengono esclusivamente a DeepCloud o ai rispettivi titolari dei diritti. Per ogni ulteriore uso dei diritti di proprietà immateriale si deve richiedere in via anticipata il consenso scritto dei titolari dei diritti. Tutte le documentazioni di DeepCloud rese accessibili nell'ambito del rapporto d'uso sono considerate proprietà intellettuale di DeepCloud.

7.9 DeepCloud è autorizzata a elaborare le foto e i video utilizzati per la procedura di identificazione o come immagine del profilo selezionata, senza alcuna pretesa di remunerazione da parte dell'utente.

8. Requisiti di utilizzo e obblighi dell'utente

8.1 L'utente dispone di un dispositivo che funge da mezzo di autenticazione autorizzato e conferma la propria identità con l'app DeepID. L'utilizzo dell'app DeepID presuppone che il dispositivo utilizzato soddisfi sempre i requisiti tecnici e di sistema necessari.

8.2 L'utente è responsabile del mezzo di autenticazione utilizzato ed utilizzabile esclusivamente da lui. Fintantoché desidera utilizzare DeepID, gli è proibito cedere il mezzo di autenticazione a terzi.

8.3 Il software del mezzo di autenticazione deve essere sempre aggiornato all'ultima versione. Occorre, in particolare, installare gli aggiornamenti messi a disposizione dal produttore (update, upgrade, service pack, hotfix, ecc.), nonché la versione di volta in volta aggiornata dell'app DeepID messa a disposizione da DeepCloud.

8.4 L'utente si impegna a sfruttare tutte le possibilità ragionevolmente esigibili e al passo con i tempi, ed a proteggere il proprio mezzo di autenticazione da attacchi e malware («virus», «worm», «trojan» e similari), in particolare utilizzando un software sempre aggiornato proveniente da fonte ufficiale.

8.5 Il mezzo di autenticazione deve essere utilizzato conformemente alle condizioni contrattuali del produttore e in modo appropriato, vanno evitate, in particolare, tutte le operazioni atte a favorire l'insorgere di rischi tramite modifica o sostituzione del software installato dal produttore del dispositivo (p. es. tramite un «jailbreak/rooting» o altro software che violi le condizioni di utilizzo prestabilite dal produttore). L'utente si impegna a installare sul proprio mezzo di autenticazione software (in particolare altre app) proveniente esclusivamente da fonti affidabili.

8.6 Il sistema operativo sul mezzo di autenticazione deve corrispondere alla versione ufficialmente messa a disposizione dal produttore ed essere compatibile con l'app DeepID, che altrimenti non sarebbe supportata. DeepID presuppone un collegamento attivo alla rete di un fornitore di servizi di telefonia mobile. Le versioni supportate del rispettivo sistema operativo sono indicate nei rispettivi app store.

8.7 L'utente è tenuto a fornire in qualsiasi momento, in occasione della procedura di identificazione e dell'utilizzo della propria identità confermata, informazioni complete, corrette e aggiornate e ad aggiornare tempestivamente eventuali modifiche. DeepCloud si riserva il diritto di richiedere prove dell'esattezza delle informazioni dell'utente e di effettuare essa stessa delle verifiche. L'obbligo di notifica riguarda in particolare le seguenti circostanze: nome, nazionalità, sesso, domicilio, dati di contatto come indirizzo e-mail, telefono, modifica del documento d'identità e del mezzo di autenticazione in caso di perdita, furto, sostituzione, nonché qualsiasi altra circostanza di fatto o di diritto che potrebbe influire sull'identificazione dell'utente e sul rapporto d'uso con DeepCloud.

8.8 Le possibilità di utilizzo dell'identità confermata tramite l'app DeepID e i relativi requisiti di utilizzo si evincono dal rispettivo contratto che l'utente stipula con DeepCloud o con un fornitore terzo.

8.9 DeepID può essere utilizzata solo per i servizi che accettano anche la sua identità confermata tramite DeepID. Inoltre, l'utente deve accettare le rispettive disposizioni contrattuali di tali servizi, che si applicano separatamente. L'utente è tenuto ad attenersi rigorosamente ad eventuali disposizioni supplementari

8.10 e a fruire di determinati servizi solo nel caso in cui soddisfi le condizioni richieste. È quindi autorizzato a incaricare un fornitore della creazione di una FEA o FEQ soltanto se abbia utilizzato i documenti d'identità all'uopo necessari per l'identificazione e disponga del domicilio richiesto. Nel caso in cui confermi quanto sopra, sebbene non corrispondi al vero, DeepCloud e i rispettivi fornitori terzi declinano qualsiasi garanzia e responsabilità per i servizi prestati, come il rilascio di una FEQ o FEA, e si riservano il diritto di intraprendere azioni legali nei confronti dell'utente. Inoltre, in tal caso, l'utente esonererà sia DeepCloud che il relativo fornitore terzo da tutte le pretese di terzi derivanti dalle informazioni errate dell'utente.

8.11 Per l'utilizzo di DeepID, la conoscenza del relativo PIN, del codice di ripristino o della protezione d'accesso del dispositivo, da un lato, e il possesso del mezzo di autenticazione, dall'altro, costituiscono elementi di sicurezza personali la cui protezione spetta all'utente.

8.12 Per garantire la protezione contro l'utilizzo improprio di DeepID e dell'identità confermata, nella scelta del PIN per DeepID o per il dispositivo non possono essere selezionate combinazioni ovvie o usuali (p. es. 123456) o combinazioni di cifre altrimenti identificabili con facilità, come numero di telefono, data di nascita, numero di targa.

8.13 L'utente è responsabile della protezione dei propri dati di accesso, in particolare della scelta di un PIN sicuro, della sicurezza del proprio codice di ripristino, nonché della protezione da accessi di terzi al mezzo di autenticazione e all'app DeepID ivi installata. Le informazioni rilevanti per la sicurezza devono essere mantenute segrete e non possono essere divulgate a terzi (compreso il rispettivo fornitore di terze parti). Eventuali registrazioni dei dati di accesso devono essere conservate in modo sicuro e separatamente dal mezzo di autenticazione, cifrate e protette dagli accessi di terzi.

8.14 Qualora l'utente sappia o abbia il fondato sospetto che un terzo sia a conoscenza dei propri dati di accesso, deve modificarli immediatamente nelle impostazioni del dispositivo e, se necessario, informare tempestivamente DeepCloud dell'accaduto.

8.15 Se il mezzo di autenticazione è stato rubato o smarrito o se l'utente sa o sospetta che un'altra persona sia venuta a conoscenza dei dati di accesso (compromissione), questi è tenuto a compiere le seguenti operazioni: deve far bloccare la DeepID comunicandolo al supporto, deve astenersi immediatamente dall'utilizzo della propria identità confermata e dei servizi che richiedono la propria autorizzazione e autenticazione, come la creazione di FEA e FEQ, deve far annullare immediatamente il certificato per la creazione di firme e, se del caso, modificare i propri dati di accesso (p. es. in DeepCloud nell'app DeepID, nell'account DeepCloud o presso il rispettivo fornitore terzo).

8.16 Non appena vengano apportate modifiche a un dispositivo utilizzato per l'autenticazione (p. es. al dispositivo stesso, all'indirizzo e-mail) o ai dati rilevanti per l'identificazione dell'utente (p. es. nome, nazionalità, altri attributi), questi informerà direttamente DeepCloud tramite le funzioni «Ho già una DeepID», «Rinnova documento» o aggiornando i dati nel proprio profilo. Qualora non riesca a farlo, dovrà rivolgersi immediatamente al supporto di DeepCloud. A quel punto, DeepCloud adotterà le misure necessarie e informerà i fornitori di servizi di certificazione o fiduciari, affinché l'identità confermata dell'utente e il certificato possano essere annullati. L'utente adotterà le misure necessarie nei confronti dei suoi altri fornitori di servizi interessati.

8.17 L'utente si impegna a verificare costantemente i dati relativi alla propria identità dopo la loro conferma e a segnalare immediatamente a DeepCloud eventuali incongruenze, nonché il sospetto di utilizzo improprio dell'identità DeepID.

8.18 All'utente è rigorosamente vietato utilizzare DeepID per scopi illeciti, ragion per cui non potrà utilizzare documenti d'identità falsificati o di terzi nell'ambito della procedura di identificazione. Qualora lo facesse, DeepCloud si riserva il diritto di vietare l'utilizzo di DeepID e di adire le vie legali nei confronti dell'utente.

8.19 In caso di violazione dei propri obblighi, l'utente si assume tutti i rischi la cui insorgenza sia favorita o causata da tale violazione.

8.20 Se l'utente non acconsente al trattamento dei dati effettuato nell'ambito di DeepID, non può utilizzare tale servizio.

8.21 L'eventualità che fornitori terzi o DeepCloud richiedano/richieda una commissione per la fornitura del servizio tramite DeepID dipende dal contratto fra l'utente e DeepCloud o il rispettivo fornitore di servizi. Possono inoltre generarsi dei costi per il trasferimento dei dati da parte del fornitore di servizi di telefonia mobile dell'utente, che sono a carico di quest'ultimo.

9. Supporto

9.1 Il supporto viene fornito da DeepCloud solo durante gli orari di assistenza usuali (p. es. sotto forma di forum o FAQ, o tramite e-mail). Per il supporto di DeepCloud occorre rivolgersi a support@deepid.swiss

9.2 In presenza di anomalie o incidenti di sicurezza durante le rispettive procedure di identificazione, di autorizzazione o autenticazione, l'utente deve rivolgersi immediatamente a DeepCloud.

9.3 DeepCloud non garantisce che le identificazioni, le autorizzazioni o le autenticazioni (come per l'incarico per una firma elettronica) possano avvenire tempestivamente in qualsiasi momento.

9.4 Anche in caso di domande riguardo ai requisiti tecnici e alle funzionalità di DeepID o in caso di anomalie nell'utilizzo, è possibile contattare il supporto.

9.5 DeepCloud si riserva di conteggiare i servizi erogati nell'ambito del supporto alle tariffe orarie di volta in volta in vigore. È possibile visualizzare i dettagli e gli orari di assistenza concreti sui siti web di DeepCloud.

10. Periodo di validità dell'identità confermata

10.1 In virtù delle condizioni di cui alle presenti CG e alle CG di DeepCloud per un account DeepCloud, l'utente può utilizzare la propria identità confermata con il mezzo di autenticazione registrato durante l'identificazione per un periodo massimo di cinque anni, per servizi di certificazione o fiduciari; tale durata si riduce di conseguenza se il periodo di validità del documento d'identità presentato dall'utente scade prima, se il certificato dei fornitori dei servizi di certificazione o fiduciari scade o se si verifica un'altra circostanza che renda necessaria una re-identificazione.

10.2 Anche per autenticazioni diverse da quelle per servizi di certificazione o fiduciari possono sussistere limitazioni temporali, anche in virtù delle condizioni di utilizzo di fornitori terzi. In tutti gli altri casi è a discrezione di DeepCloud stabilire la durata di utilizzo di un'identificazione confermata, inclusa una re-identificazione dell'utente eventualmente necessaria.

11. Protezione dei dati e riservatezza

11.1 DeepCloud si atterrà alle disposizioni del diritto sulla protezione dei dati applicabile nell'ambito del proprio trattamento dei dati. DeepCloud definisce, nella sua sfera di responsabilità, la propria struttura aziendale in modo tale da soddisfare le esigenze particolari in materia di protezione dei dati. Essa adotta misure tecniche e organizzative atte a garantire un'adeguata protezione dei dati dell'utente da abusi e perdite, conformemente ai requisiti del diritto sulla protezione dei dati.

11.2 DeepCloud tratterà con riservatezza tutte le informazioni non generalmente note di cui viene a conoscenza in merito all'utente e alle sue relazioni commerciali. Essa renderà tali informazioni accessibili a terzi solo se e nella misura consentita dal rapporto d'uso o dalla legge, se l'utente lo ha espressamente autorizzato o qualora ciò si renda necessario in virtù di un ordine delle autorità o di un ordine giudiziario, nonché in virtù di un obbligo legale. Garantisce altresì il rispetto dell'obbligo di riservatezza di tutti i collaboratori e dei terzi coinvolti nel presente rapporto d'uso.

11.3 DeepCloud raccoglie, memorizza e tratta, oltre ai dati raccolti conformemente alle norme vigenti e necessari per la fornitura di un servizio di certificazione o fiduciario, tutti i dati e le informazioni necessari per la fornitura dei propri servizi all'utente. Il trattamento di tali dati è disciplinato, oltre che dalle leggi applicabili, anche dalle direttive sui certificati per i servizi di certificazione o fiduciari.

11.4 DeepCloud si avvale di terzi per i propri servizi nell'ambito dell'identificazione dell'utente. Si tratta in proposito di un trattamento di dati delegato per conto di DeepCloud. DeepCloud ha stipulato con tali terzi i contratti all'uopo necessari in materia di protezione dei dati.

11.5 Il trattamento dei dati personali di DeepCloud è descritto nell'informativa sulla protezione dei dati riportata sul relativo sito web. Si applica la versione pubblicata di volta in volta in vigore.

11.6 Sulla base dei dati forniti dall'utente nell'ambito della procedura di identificazione e raccolti da DeepCloud, il rispettivo fornitore di un servizio di certificazione o fiduciario rilascia, su richiesta e con manifestazione di volontà dell'utente, un certificato qualificato o avanzato contenente le informazioni necessarie sull'utente.

11.7 DeepCloud conserva i dati sopra descritti e i mezzi con cui è stata verificata l'identità conformemente agli obblighi contrattuali e legali di conservazione, anche al fine di permettere all'utente di usufruire di un servizio di certificazione o fiduciario. Il periodo di conservazione per la FEQ, secondo la FiEle, è di 11 anni, mentre, secondo il regolamento eIDAS, è di 30 anni; nel caso della FEA, sia secondo la FiEle che secondo il regolamento eIDAS, il termine è di 7 anni. In virtù del periodo di validità massimo di un'identificazione pari a 5 anni, incluso un ulteriore periodo di sicurezza di un anno, ciò comporta periodi di conservazione per la FEQ fino a un massimo di 17 anni secondo la FiEle, e fino a un massimo di 36 anni secondo il regolamento eIDAS; mentre per la FEA, il periodo di conservazione arriva fino a 13 anni, sia secondo la FiEle che secondo il regolamento eIDAS.

11.8 Tali periodi di conservazione garantiscono che la verificabilità della correttezza di un documento firmato elettronicamente possa essere mantenuta negli anni successivi alla sua creazione. A tal fine, tutte le informazioni pertinenti relative ai dati emessi e ricevuti vengono registrate e conservate in modo tale da essere disponibili, in particolare per poter fornire le relative prove nell'ambito di procedure giudiziarie e garantire la continuità del servizio di certificazione o fiduciario.

11.9 DeepCloud cancella i dati necessari non prima che siano decorsi 17 anni, secondo la FiEle, e 36 anni, secondo il regolamento eIDAS, dall'esecuzione della procedura di identificazione. In caso di identificazione solo ai fini del rilascio di una FEA, DeepCloud cancella tali dati non prima che siano decorsi 13 anni dall'esecuzione della procedura di identificazione, sia secondo la FiEle che secondo il regolamento eIDAS. La cancellazione dei dati può avvenire solo dopo la scadenza degli obblighi di conservazione esistenti.

11.10 Al fine di informare l'utente della scadenza del periodo di validità dell'identità confermata e di un'eventuale autorizzazione alla firma, DeepCloud memorizza la data in cui ciò accadrà e ne informa l'utente per iscritto o in altro modo (p. es. sulla sua app DeepID, in un suo account DeepCloud esistente o tramite e-mail), affinché l'utente possa procedere tempestivamente ad una re-identificazione. Con la presente, l'utente vi acconsente espressamente.

11.11 Qualora i dati possano essere necessari per difendere fornitori terzi o DeepCloud da eventuali pretese di risarcimento dei danni, questi verranno conservati per la durata di eventuali termini di prescrizione.

11.12 L'utente può autorizzare, per vari scopi, la trasmissione di dati, documenti e informazioni a terzi nell'ambito di un'autenticazione tramite DeepID, avvalendosi o meno di servizi di fornitori terzi, come la trasmissione di dati a un potenziale datore di lavoro, un'assicurazione o una banca. Può inoltre utilizzare la propria identità confermata per autenticarsi come persona autorizzata alla rappresentanza di un'organizzazione. Le disposizioni sulla protezione dei dati di fornitori terzi indicano le modalità con cui tali fornitori terzi trattano i dati dell'utente e le possibilità che ha l'utente di influire su tale trattamento dei dati. DeepCloud non risponde di tali trattamenti dei dati.

12. Ricorso a terzi

12.1 Con la presente l'utente autorizza DeepCloud a ricorrere in qualsiasi momento a terzi per il regolare adempimento dei propri obblighi. Questi terzi vengono selezionati con cura e incaricati da DeepCloud. Essi sono vincolati a istruzioni e sottoposti regolarmente a controlli. Ci si avvale, in particolare, di fornitori di hosting e di servizi con soluzioni server in Svizzera e con sede sociale in Svizzera o nell'UE.

13. Garanzia

13.1 DeepCloud offre all'utente una fedele e accurata esecuzione dei propri servizi ai sensi delle presenti CG.

13.2 DeepCloud non garantisce un funzionamento ininterrotto o indisturbato di DeepID (inclusa l'app DeepID) e l'utilizzo delle relative funzionalità, né in generale né in un determinato momento. Si declina, nella misura consentita dalla legge, qualsiasi garanzia per DeepID (inclusi app, software, hosting, utilizzati, ecc.). DeepID viene messa a disposizione «così com'è».

13.3 DeepCloud si adopera affinché DeepID sia messa a disposizione ininterrottamente. Tuttavia, non è possibile garantirne una disponibilità ininterrotta. DeepCloud può, in qualsiasi momento, limitare o interrompere temporaneamente la disponibilità di DeepID, soprattutto se necessario alla luce dei limiti di capacità, della sicurezza o dell'integrità dei server o ai fini dell'esecuzione di misure tecniche di manutenzione o riparazione o della fornitura regolare o ottimizzata dei servizi. Si impegna, a tal fine, a tener conto degli interessi dell'utente e, nella misura del possibile, informerà quest'ultimo di eventuali interruzioni con un adeguato preavviso.

13.4 I servizi erogati gratuitamente sono forniti senza alcuna pretesa di adempimento o di garanzia. DeepCloud può, in qualsiasi momento e senza preavviso, sospendere o modificare servizi forniti gratuitamente o può offrirli solo a fronte di pagamento. Ciò non determina l'insorgere di pretese o diritti dell'utente.

13.5 Non sussistono garanzie che DeepID soddisfi le esigenze individuali dell'utente, indipendentemente dal fatto che tali esigenze siano state comunicate o meno a DeepCloud. Le informazioni sul sito web di DeepCloud o altre indicazioni di carattere pubblicitario di DeepCloud non costituiscono indicazioni di qualità o garanzie.

13.6 DeepCloud, in qualità di servizio di registrazione, deve soddisfare con la procedura di identificazione, quale componente di un servizio di certificazione o fiduciario, i requisiti posti a tali servizi dalla legge e dagli standard tecnici. A tal proposito, DeepCloud adotta misure di sicurezza adeguate e conformi allo stato attuale della tecnica. DeepCloud è responsabile della valutazione e della specificazione dei requisiti previsti dalle leggi e dai regolamenti applicabili.

13.7 L'utente prende atto del fatto che, nonostante tutti gli sforzi profusi da DeepCloud, l'impiego di tecnologie e standard di sicurezza moderni e il controllo da parte di un organismo indipendente del rispetto degli standard tecnici e delle prescrizioni legali, non è possibile garantire una sicurezza assoluta e ineccepibile del processo di identificazione e dei servizi di certificazione o fiduciari.

13.8 DeepCloud non garantisce che un'identificazione, una verifica, un'autorizzazione o un'autenticazione possano essere eseguite e concluse in qualsiasi momento e, nella misura consentita dalla legge, declina qualsiasi responsabilità per eventuali danni dovuti a identificazioni, verifiche, autorizzazioni o autenticazioni tardive, omesse o non concluse con successo.

14. Responsabilità e forza maggiore

14.1 DeepCloud risponde solo in caso di dolo e negligenza grave, nonché per danni a persone. Per il resto, è espressamente esclusa qualsiasi ulteriore responsabilità, in particolare quella per colpa lieve, danni conseguenti, danni patrimoniali, danni immateriali e indiretti (come la perdita totale o parziale di documenti o dati, spese supplementari, mancato guadagno, danni dovuti a interruzioni della disponibilità, rivendicazioni di terzi, ecc.) nonché per gli ausiliari (inclusi terzi coinvolti). Ciò vale anche per un'eventuale responsabilità oggettiva.

14.2 DeepCloud non si assume alcuna responsabilità per la disponibilità costante dell'app DeepID, del proprio supporto, delle procedure e delle possibilità di impiego offerte, nonché delle singole funzionalità dell'app DeepID.

14.3 DeepCloud non risponde nei confronti dell'utente per il corretto funzionamento dei sistemi di terzi, in particolare per l'hardware e il software utilizzati dall'utente o per un servizio di terzi da questi fruito utilizzando la propria identità confermata per l'autenticazione.

14.4 Non sussiste alcuna responsabilità se l'erogazione della prestazione è temporaneamente interrotta, parzialmente o totalmente limitata o impossibile per cause di forza maggiore. Sono considerati cause di forza maggiore specificatamente eventi naturali di particolare intensità (valanghe, inondazioni, frane ecc.), eventi bellici, tumulti, restrizioni impreviste da parte delle autorità, nonché pandemie o epidemie. Qualora DeepCloud non sia in grado di adempiere ai propri obblighi, il loro adempimento o il termine per l'adempimento viene differito conseguentemente all'evento verificatosi. DeepCloud non risponde di eventuali danni causati all'utente dal differimento dell'adempimento.

14.5 Il detentore deve far valere eventuali pretese entro sei mesi dall'erogazione delle prestazioni.

14.6 Le presenti esclusioni e limitazioni di responsabilità si applicano alle pretese contrattuali ed extra-contrattuali del detentore.

14.7 DeepCloud non risponde dei danni derivanti dall'utilizzo illecito o non conforme ai termini del contratto di DeepID da parte dell'utente.

14.8 Sono esclusi da tali limitazioni ed esclusioni di responsabilità i regolamenti imperativi in materia di responsabilità basati su leggi sulla responsabilità dei prodotti, leggi sulla protezione dei consumatori, regolamenti FiEle o eIDAS, nonché sulle loro leggi di attuazione. Vigono in tal caso, anche per DeepCloud, le limitazioni ed esclusioni di responsabilità eventualmente previste in tali disposizioni.

14.9 DeepCloud ha disciplinato la propria responsabilità nei confronti dell'utente riguardo all'utilizzo di DeepSign nelle proprie condizioni generali per l'utilizzo dell'account DeepCloud e dei DeepServices.

14.10 L'utente risponde segnatamente per DeepCloud e la esonera da qualsiasi pretesa (di risarcimento dei danni) in relazione all'utilizzo di DeepID, basata sulla violazione di leggi e regolamenti applicabili, del buon costume, delle presenti CG o delle disposizioni contrattuali di DeepCloud o di fornitori terzi, come i fornitori di servizi di certificazione o fiduciari.

15. Modifiche delle presenti CG

15.1 DeepCloud si riserva il diritto di modificare e completare in qualsiasi momento l'app DeepID e le presenti CG. In particolare, in caso di modifiche della FiEle, del regolamento eIDAS e delle rispettive leggi di attuazione, nonché in caso di disposizioni dell'organismo competente per il riconoscimento, la conferma e la vigilanza o di un organismo indipendente per la verifica delle firme, i fornitori di servizi di certificazione o fiduciari possono essere costretti ad adattare le direttive esistenti in materia di certificati e, di conseguenza, DeepCloud, in qualità di servizio di registrazione, ad adattare le presenti CG. L'utente viene informato da DeepCloud di eventuali modifiche prima della loro entrata in vigore o, in caso di utilizzo di un servizio, gli vengono comunicate le disposizioni di volta in volta in vigore. Tali informazioni possono essere comunicate all'utente in modo appropriato.

15.2 Le modifiche sono considerate accettate se l'utente non disdice il rapporto contrattuale entro l'entrata in vigore delle nuove DG, ma in ogni caso al momento dell'utilizzo di DeepID dopo l'entrata in vigore delle nuove disposizioni, nonostante la possibilità di prendere atto delle modifiche.

15.3 L'utente può anche rifiutare di accettare le nuove condizioni rinunciando all'utilizzo di DeepID (così come all'identità confermata, alle autorizzazioni e alle autenticazioni tramite DeepID) conformemente alle presenti CG, a partire dall'entrata in vigore delle condizioni modificate.

15.4 Qualora singole disposizioni delle presenti CG dovessero rivelarsi inefficaci o nulle, ciò non comporterà l'inefficacia o la nullità delle altre disposizioni, ma saranno sostituite da disposizioni che si avvicinano il più possibile allo scopo economico di quelle sostituite. Lo stesso vale in caso di lacuna nelle condizioni di utilizzo.

16. Entrata in vigore, durata e cessazione

16.1 Il rapporto d'uso con l'utente relativamente a DeepID si instaura con l'accettazione delle presenti CG all'interno dell'app DeepID e sussiste a tempo indeterminato.

16.2 DeepCloud è autorizzata a disdire il rapporto d'uso in qualsiasi momento, senza indicarne i motivi. Al momento della disdetta, DeepCloud bloccherà l'accesso a DeepID e all'identità DeepID confermata, ne interromperà l'utilizzo e cesserà la comunicazione tecnica con i DeepServices o con servizi di fornitori terzi. Ciò significa, in particolare, che tutti i servizi ancora in sospeso, nonché i messaggi di stato e le informazioni eventualmente correlati, non vengono più trasportati o eseguiti né saranno più disponibili.

16.3 L'utente può rinunciare in qualsiasi momento all'utilizzo di DeepID e cancellare l'app DeepID dal proprio mezzo di autenticazione. Spetta all'utente stesso programmare la cessazione dell'utilizzo di DeepID e della propria identità DeepID. Per quanto riguarda il blocco della propria identità DeepID o la cancellazione dei dati, l'utente si rivolge a DeepCloud.

16.4 Al momento della cessazione del rapporto d'uso, l'utente non ha più a disposizione la propria identità confermata né può più utilizzare DeepID.

17. Diritto applicabile e foro competente

17.1 Tutti i rapporti giuridici in relazione alle presenti CG sono soggetti al diritto svizzero con esclusione delle norme del diritto internazionale privato e della Convenzione di Vienna sui contratti compravendita internazionale di merce, indipendentemente dal fatto che un utente utilizzi DeepID nella propria qualità di consumatore o per conto di un'impresa.

17.2 Qualora l'utente sia un consumatore con dimora abituale nell'UE/nel SEE, trova altrimenti applicazione, a titolo complementare, la legge imperativa sulla tutela dei consumatori dello Stato UE/SEE in cui risiede abitualmente. Lo stesso vale qualora si tratti di un Paese soggetto all'applicazione del regolamento eIDAS.

17.3 Fermi restando i fori imperativi, per tutte le controversie derivanti dalle o correlate alle presenti CG, il foro competente esclusivo è la città di San Gallo.

18. Disposizioni finali

18.1 L'utente non può trasferire a terzi alcun diritto derivante dal presente rapporto d'uso. DeepCloud è autorizzata a trasferire a terzi tutti i diritti e doveri derivanti dal presente rapporto d'uso. L'utente acconsente con la presente a un'eventuale cessione o un eventuale trasferimento.

18.2 In caso di controversie, le parti si adoperano per favorire una risoluzione amichevole della controversia.

18.3 Tutte le designazioni di persone nelle presenti CG devono essere intese come applicabili a entrambi i generi.

18.4 Le presenti CG sono disponibili in diverse lingue. In caso di divergenze o contraddizioni fa fede la versione tedesca.

19. Legge imperativa sulla tutela dei consumatori dell'UE/SEE

19.1 Il termine di opposizione riguardo alle modifiche delle presenti CG per utenti a cui si applica a titolo complementare la legge imperativa sulla tutela dei consumatori dell'UE/SEE è di 4 settimane.

19.2 DeepCloud può disdire in via ordinaria il rapporto d'uso in qualsiasi momento per la fine del mese, con un termine di disdetta di 30 giorni.

19.3 Se l'utente è un consumatore nell'UE/SEE, DeepCloud non è disposta né tenuta a partecipare a una procedura di risoluzione delle controversie dinanzi a un organismo di conciliazione per consumatori. Informativa ai consumatori a norma del regolamento (UE) n. 524/2013: ai fini della risoluzione stragiudiziale delle controversie relative ai consumatori, la Commissione europea ha istituito una piattaforma per la risoluzione online delle controversie (piattaforma ODR). La piattaforma ODR è raggiungibile al link https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.home2.show&lng=IT.