Accordo sulla Protezione dei Dati (DPA)

Le parti concludono il presente Accordo sul Protezione dei dati("DPA"), che fa parte dell'Accordo tra il Cliente e il Fornitore ("Glarish, Inc"), ovvero il Contratto SaaS di Digital Signage (il "Contratto") per riflettere il loro accordo sul Protezione dei dati personali, in conformità con i requisiti delle leggi e dei regolamenti sulla protezione dei dati, incluso il GDPR e il CCPA nella misura applicabile. Nella misura in cui il Fornitore, nel fornire i Servizi stabiliti nel Contratto, elabora i Dati personali per conto del Cliente, si applicano le disposizioni del presente DPA.

I riferimenti al Contratto saranno interpretati come comprendenti questo DPA. Tutti i termini in maiuscolo non definiti nel presente documento avranno i rispettivi significati loro attribuiti nel Contratto.

Questo DPA è costituito da due parti: (i) il corpo principale di questo DPA e (ii) gli allegati 1, 2, 3 e 4 del presente documento.

ESECUZIONE DEL DPA

Per completare questo DPA, il cliente deve:

a. Firmare il corpo principale di questo DPA nella casella della firma sottostante.

b. Completare le informazioni mancanti e firmare l'Allegato 1, l'Allegato 2, l'Allegato 3 e l'Allegato 4. L'Allegato 4 si applica, nel caso di un Titolare del Protezione dei dati nell'ambito dell'Articolo 3 GDPR.

Invia il DPA compilato e firmato al Fornitore tramite e-mail a support@glarish.com. Al ricevimento di un DPA validamente compilato, questo DPA sarà legalmente vincolante (a condizione che il Cliente non abbia sovrascritto o modificato nessuno dei termini oltre a completare le informazioni mancanti).

COME SI APPLICA IL DPA

Se l'entità cliente che firma questo DPA è una parte dell'Accordo, allora questo DPA è un'aggiunta e forma parte dell'Accordo.

Se l'entità cliente che firma questo DPA ha presentato l'Allegato A ai sensi dell'Accordo, allora questo DPA è un'aggiunta a tale Programma A e ai termini di rinnovo applicabili.

Se l'entità cliente che firma questo DPA non è una parte dell'accordo, questo DPA non è valido e non è legalmente vincolante. Tale entità dovrebbe richiedere che l'entità cliente che è parte dell'accordo esegua questo DPA.

Se l'entità cliente che firma il DPA non è una parte dell'accordo direttamente con il fornitore, ma è invece un cliente indirettamente tramite un rivenditore autorizzato o un partner, questo DPA non è valido e non è legalmente vincolante. Tale entità deve contattare il Rivenditore autorizzato o il Partner per discutere se sia necessaria una modifica al suo accordo con quel Rivenditore o Partner.

Il presente DPA non sostituirà alcun diritto analogo o aggiuntivo relativo al Protezione dei dati personali contenuto nel Contratto.

TERMINOLOGIA PER LA PROTEZIONE DEI DATI

Il Cliente e Glarish accettano le seguenti disposizioni in relazione a qualsiasi Cliente di Dati Personali elaborato da Glarish in relazione alla fornitura dei Servizi ai sensi del Contratto.

1. DEFINIZIONI

"Decisione di adeguatezza" indica una decisione della Commissione europea secondo la quale un paese terzo o un'organizzazione internazionale garantisce un livello adeguato di protezione dei dati ai

sensi dell'articolo 45 (9) GDPR in combinazion con quanto disposto con l'articolo 25 (6) della direttiva 95/46 / CE, o ai sensi dell'articolo 45, paragrafo 3, del GDPR, a seconda dei casi;

"Affiliato" indica, in relazione a qualsiasi entità, qualsiasi altra entità che controlla, controllata da o sotto controllo comune con tale entità, solo per il tempo in cui tale controllo esiste;

"Affiliato autorizzato" indica qualsiasi Affiliato / i del Cliente, che (i) è soggetto alle Regole aziendali vincolanti del Cliente oa clausole contrattuali simili, comprese le clausole contrattuali standard o le clausole contrattuali approvate da un'Autorità di vigilanza, ove applicabile, con il Cliente a garantire un livello adeguato di protezione dei Dati personali, (ii) non è stabilito in un Paese terzo soggetto a restrizioni e (iii) è autorizzato a utilizzare i Servizi ai sensi dell'Accordo tra Cliente e Fornitore, ma non è una Parte firmataria dell'Accordo e non è un "Cliente" come definito nel Contratto;

"Dati comportamentali" indica i dati che tracciano o in altro modo monitorano le attività online di un interessato o l'utilizzo di prodotti e servizi da parte dell'interessato;

Le "Norme aziendali vincolanti" sono norme interne vincolanti che regolano il trasferimento di Dati personali all'interno di un'organizzazione che, ove applicabile, è stata approvata dalle autorità per la protezione dei dati dell'UE in quanto fornisce un livello adeguato di protezione ai Dati personali;

"CCPA" indica il California Consumer Privacy Act (CODICE CAL. CIV. § 1798.100 e segg.) E le relative norme di attuazione.

"Controllo" indica la proprietà diretta o indiretta di oltre il 50% del capitale di voto o un diritto simile di proprietà di un'entità, o il potere legale di dirigere o determinare la direzione della gestione generale e delle politiche di tale entità, sia attraverso il proprietà del capitale votante, per contratto o altro. Controllo e Controllo devono essere interpretati di conseguenza;

"Dashboard" per i Servizi applicabili, indica le funzionalità dell'interfaccia utente del Software ospitato (come descritto nel Contratto);

"Titolare del trattamento" indica l'entità che determina le finalità e i mezzi del Protezione dei dati personali, come definito nel GDPR, e ha lo stesso significato di "business", poiché tale termine è definito dal CCPA;

"Responsabile del trattamento" indica l'entità che elabora i dati personali per conto del titolare del trattamento, come definito nel GDPR, e ha lo stesso significato di "fornitore di servizi", poiché tale termine è definito dal CCPA;

"Leggi e regolamenti sulla protezione dei dati" indica tutte le leggi e i regolamenti applicabili al Protezione dei dati personali come parte di o in connessione con i Servizi, inclusi ma non limitati a (i) leggi e regolamenti dell'Unione Europea, dello Spazio economico europeo e i loro stati membri, incluso il GDPR, e ii) le decisioni di adeguatezza come (i) o (ii) possono essere modificate e sono in vigore di volta in volta;

"Soggetto dei dati" indica la persona a cui si riferiscono i Dati personali, come definito nel GDPR, e ha lo stesso significato di "consumatore" come tale termine è definito nel CCPA;

"GDPR" indica il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, sulla protezione delle persone fisiche con riguardo al Protezione dei dati personali e sulla libera circolazione di tali dati, e che abroga la Direttiva 95 / 46 / CE (Regolamento generale sulla protezione dei dati), che può essere modificato di volta in volta;

"Glarish" indica il Fornitore;

"Dati personali" indica i dati su una persona fisica elaborata da Glarish in relazione alla fornitura dei Servizi ai sensi del Contratto, da cui tale persona è identificata o identificabile, come definito nel GDPR; A scanso di equivoci, i Dati personali includono ma non sono limitati a Dati di supporto, Dati comportamentali e Dati identificativi univoci e hanno lo stesso significato di "informazioni personali" come tale termine è definito dal CCPA;

"Elaborazione" indica qualsiasi operazione o insieme di operazioni eseguite sui Dati personali, anche con mezzi automatici, come raccolta, registrazione, organizzazione, conservazione, adattamento o alterazione, recupero, consultazione, utilizzo, divulgazione mediante trasmissione, diffusione, trasferire o rendere disponibili in altro modo, allineamento o combinazione, blocco, cancellazione o distruzione;

"Paese terzo soggetto a restrizioni" indica un paese verso il quale il trasferimento di dati personali o dal quale l'accesso ai dati personali sarebbe vietato dalle leggi e dai regolamenti applicabili sulla protezione dei dati;

"Clausole contrattuali standard" indica le clausole contrattuali adottate dalla Commissione europea sulla base dell'articolo 46 (5) GDPR in combinato disposto con l'articolo 26 (4) della direttiva 95/46 / CE, o ai sensi dell'articolo 46 (2) c) o d) GDPR, ove applicabile.

"Software" indica la versione in codice oggetto del software GLARISH e / o qualsiasi software a cui il Cliente ha accesso come parte dei Servizi, inclusi eventuali aggiornamenti o nuove versioni;

"Fornitore" indica l'entità Glarish, che è parte di questo DPA e dell'Accordo, ovvero Glarish, Inc., Una società con sede negli Stati Uniti, con sede legale in 30 Regalo Drive, Mission Viejo, California, 92692.

"Responsabili" indica qualsiasi Responsabile del protezione dei dati non affiliato o affiliato, incaricato da Glarish, che accetta di ricevere da Glarish o da qualsiasi altro Responsabile del Protezione dei dati personali di Glarish destinati esclusivamente al trattamento da eseguire per conto del Cliente , in conformità con le sue istruzioni, i termini del presente DPA e i termini del contratto scritto del Responsabile;

"Autorità di vigilanza" indica un'autorità pubblica indipendente istituita da uno Stato membro dell'UE, ai sensi del GDPR;

"Dati di supporto" indica le informazioni che Glarish raccoglie, quando il Cliente invia una richiesta di servizi di supporto o altra risoluzione dei problemi, comprese le informazioni su hardware, software e altri dettagli relativi all'incidente di supporto, come le informazioni di autenticazione, le informazioni sulle condizioni del prodotto, dati di sistema e registro relativi a installazioni software e configurazioni hardware e file di rilevamento degli errori;

"Dati identificativi univoci" indica un identificatore persistente univoco associato a un individuo o a un dispositivo in rete, incluso un numero cliente contenuto in un cookie, un ID utente, un numero di serie del processore o un numero di serie del dispositivo.

2. TRATTAMENTO DEI DATI PERSONALI

2.1 Ruoli delle parti. Le parti riconoscono e accettano che ai fini del presente DPA il Cliente è il Titolare del trattamento e il Fornitore è il Responsabile del trattamento, che il Fornitore si impegna nell'elaborazione, ovvero nel funzionamento, nella manutenzione e nel supporto dei Servizi, compresa la funzione di super amministratore per gli account in Glarish Software, Glarish ha il diritto di assumere subincaricati del trattamento in conformità ai requisiti stabiliti nella clausola 5 di questo DPA. Il Cliente può consentire l'utilizzo dei Servizi agli Affiliati autorizzati in conformità alle condizioni stabilite nelle Clausole 14 e 15 di questo DPA.

2.2 Protezione dei dati personali da parte del cliente. Il Cliente, nell'utilizzo dei Servizi, elaborerà i Dati personali in conformità con le leggi e i regolamenti sulla protezione dei dati. A scanso di equivoci, le istruzioni del Cliente al Glarish per il Protezione dei dati personali devono essere conformi alle leggi e ai regolamenti sulla protezione dei dati. Inoltre, il Cliente sarà l'unico responsabile per l'accuratezza, l'affidabilità, la qualità e la legalità dei Dati personali e dei mezzi con cui il Cliente ha acquisito i Dati personali, inclusa la fornitura di eventuali comunicazioni richieste e l'ottenimento del consenso necessario da parte dei suoi dipendenti, agenti, o terze parti a cui estende i vantaggi dei Servizi o i cui Dati Personali vengono elaborati nell'Utilizzo dei Servizi da parte del

Cliente. Si afferma espressamente che il Cliente è l'unico responsabile (i) della legalità delle finalità del Trattamento, (ii) della necessità del Trattamento per servire a tali finalità, (iii) di informare tutti gli Interessati, i cui Dati Personali viene elaborato utilizzando i Servizi, sulla portata, lo scopo, la durata e le modalità del Trattamento, i loro diritti rispetto al Trattamento (iv) acquisire il consenso degli Interessati, i cui Dati Personali sono oggetto di trattamento utilizzando i Servizi, ove applicabile v) per condurre uno studio di valutazione dell'impatto sulla protezione dei dati (DPIA) ai sensi degli articoli 35 e 36 del GDPR, ove applicabile.

2.3 Elaborazione dei dati personali da parte di Glarish.

un. Glarish tratterà i dati personali come informazioni riservate e tratterà i dati personali solo per conto e in conformità con le istruzioni documentate del cliente per i seguenti scopi: (i) elaborazione in conformità con il contratto e questo DPA; (ii) Elaborazione avviata da Affiliati Autorizzati o Utenti Autorizzati nell'utilizzo del Servizio; e (iii) Elaborazione per conformarsi ad altre istruzioni documentate e ragionevoli fornite dal Cliente (ad esempio, tramite e-mail) laddove tali istruzioni siano coerenti con i termini del Contratto. b. Il Cliente si assume la piena responsabilità di mantenere la quantità di Dati personali forniti a Glarish al minimo necessario per l'esecuzione dei Servizi. c. Glarish non sarà tenuta a rispettare o osservare le istruzioni del Cliente, se tali istruzioni violano il GDPR, il CCPA o le leggi e i regolamenti sulla protezione dei dati. Glarish informerà immediatamente il Cliente se, a suo parere, un'istruzione viola il GDPR o il CCPA o le leggi e i regolamenti sulla protezione dei dati. d. Glarish tratterà i Dati personali, se richiesto dalla legislazione dell'Unione Europea o dello Stato membro a cui Glarish è soggetto; in tal caso, Glarish informerà il Cliente di tale requisito legale prima dell'elaborazione, a meno che tale legge non vieti tali informazioni per importanti motivi di interesse pubblico. Glarish informerà tempestivamente il Cliente di qualsiasi richiesta legalmente vincolante di divulgazione di Dati personali da parte di un'autorità di contrasto, salvo diversamente vietato, come un divieto ai sensi del diritto penale di preservare la riservatezza di un'indagine delle forze dell'ordine.

2.4 Ambito del trattamento. L'oggetto della Protezione dei dati personali da parte di Glarish è la prestazione dei Servizi ai sensi del Contratto. La durata del Trattamento, la natura e la finalità del Trattamento, i tipi di Dati Personali e le categorie di Interessati trattati ai sensi del presente DPA sono ulteriormente specificati nell'Allegato 1 al presente DPA.

3. RIGHTS OF DATA SUBJECTS

3.1 Reclami o comunicazioni relativi ai dati personali. Nel caso in cui Glarish riceva reclami, avvisi o comunicazioni ufficiali relativi alla Protezione dei dati personali per o per conto del Cliente o alla conformità di una delle parti alle leggi e ai regolamenti sulla protezione dei dati, nella misura consentita dalla legge, Glarish informerà tempestivamente il Cliente e, nella misura applicabile, Glarish fornirà al Cliente cooperazione e assistenza commercialmente ragionevoli in relazione a tali reclami, avvisi o comunicazioni. Il Cliente sarà responsabile per qualsiasi costo ragionevole derivante dalla fornitura di tale assistenza da parte di Glarish.

3.2 Richieste dell'interessato. Nella misura consentita dalla legge, Glarish informerà tempestivamente il Cliente, se Glarish riceve una richiesta da un Soggetto interessato di esercitare il diritto dell'interessato al consenso e di revocare il consenso, diritto di accesso, diritto di rettifica, limitazione dell'elaborazione, cancellazione ("Diritto all'oblio"), alla portabilità dei dati, all'opposizione al Trattamento o al suo diritto a non essere soggetto a un processo decisionale individuale automatizzato ("Richiesta dell'interessato") e, a scanso di equivoci, richieste simili a quanto previsto dal CCPA. Tenendo conto della natura del Trattamento, Glarish assisterà il Cliente con misure organizzative e tecniche appropriate, nella misura in cui ciò è possibile, per l'adempimento dell'obbligo del Cliente di rispondere a una richiesta del Soggetto interessato ai sensi delle leggi e dei regolamenti sulla protezione dei dati. Inoltre, nella misura in cui il Cliente, nel suo utilizzo dei Servizi, non ha la capacità di rispondere a una Richiesta dell'Interessato, Glarish, su richiesta del Cliente, fornirà sforzi commercialmente ragionevoli per assistere il Cliente nel rispondere a tale Richiesta dell'Interessato,

nella misura in cui Glarish è legalmente autorizzato a farlo e la risposta a tale richiesta del soggetto dei dati è richiesta dalle leggi e dai regolamenti sulla protezione dei dati. Nella misura consentita dalla legge, il Cliente sarà responsabile di eventuali costi derivanti dalla fornitura di tale assistenza da parte di Glarish.

4. DIPENDENTI GLARISH

4.1. Riservatezza. Glarish garantisce che il proprio personale impegnato nel Protezione dei dati personali sia informato della natura riservata dei dati personali, abbia ricevuto una formazione adeguata sulle proprie responsabilità e abbia sottoscritto accordi di riservatezza scritti. Glarish deve garantire che tali obblighi di riservatezza sopravvivano alla cessazione del rapporto di lavoro con il personale.

4.2. Affidabilità. Glarish adotterà misure commercialmente ragionevoli per garantire l'affidabilità del proprio personale impegnato nel Protezione dei dati personali.

4.3. Limitazione di accesso. Glarish garantirà che l'accesso di Glarish ai Dati personali sia limitato al personale che assiste nella fornitura dei Servizi in conformità con l'Accordo e che l'accesso sia limitato al personale necessario per la fornitura dei Servizi.

4.4. Responsabile della protezione dei dati. Glarish nominerà, un responsabile della protezione dei dati, se e per cui tale nomina è richiesta dall'articolo 37 del GDPR. Qualsiasi persona nominata e il personale di Glarish responsabile per le questioni relative alla privacy possono essere contattati all'indirizzo privacy@glarish.com**.**

5. RESPONSABILI

5.1 Nomina di Responsabili. Il cliente riconosce e accetta che:

i. Glarish ha il diritto di mantenere i suoi affiliati attuali e futuri come Responsabili. Glarish informerà il Cliente di eventuali modifiche previste alle proprie Affiliate, che agiscono in qualità di Responsabili.

ii. Glarish può di volta in volta coinvolgere terze parti per elaborare i dati personali in relazione alla fornitura dei servizi.

5.2 Elenco dei Responsabili. Gli attuali Subincaricati non affiliati sono elencati nell'Allegato 3 a questo DPA e il Cliente autorizza l'uso di tali Subincaricati per assistere Glarish nell'adempimento degli obblighi di Glarish ai sensi del Contratto e di questo DPA. Glarish informerà il Cliente di eventuali modifiche previste a tale Elenco inviando un'e-mail. Inoltre, l'elenco dei Subincaricati non affiliati è disponibile anche nella sezione dei servizi.

5.3. Diritto di opposizione per nuovi Responsabili. Il Cliente, al fine di esercitare il proprio diritto di opporsi all'uso da parte del Fornitore di un nuovo Responsabile, affiliato o meno, dovrà informare tempestivamente il Fornitore per iscritto entro dieci (10) giorni lavorativi dal ricevimento della notifica del Fornitore sulla sua intenzione di utilizzare un nuovo Responsabile. I Dati Personali non saranno in alcun modo trattati dal Responsabile contro il quale il Cliente si è espressamente opposto. Se il Fornitore e il Cliente non riescono a trovare una risoluzione reciprocamente accettabile per affrontare l'obiezione del Cliente entro un periodo di tempo ragionevole, che non deve superare i trenta (30) giorni, il Cliente può interrompere i Servizi. Il Fornitore rimborserà al Cliente eventuali tariffe prepagate che coprono il resto del Servizio dopo la data di effettiva cessazione rispetto a tale Servizio terminato. Il Cliente dovrà restituire a proprie spese di spedizione qualsiasi hardware (ad es. media player GLARISH) fornito da Glarish tramite i rivenditori autorizzati.

5.4. Rapporti contrattuali. Glarish impegnerà e divulgherà i Dati personali solo a Subincaricati non affiliati che sono parti di accordi scritti con Glarish contenenti obblighi di protezione dei dati non meno protettivi degli obblighi di questo DPA. Glarish accetta e garantisce, su richiesta del Cliente, di

inviare prontamente una copia di qualsiasi contratto del Responsabile al Cliente e di mettere a disposizione dell'Interessato su richiesta una copia del DPA, o di qualsiasi contratto di elaborazione esistente, a meno che il Il DPA o il contratto contengono informazioni commerciali, nel qual caso può rimuovere tali informazioni commerciali, ad eccezione dell'Allegato 2, che deve essere sostituito da una descrizione sintetica delle misure di sicurezza, nei casi in cui l'Interessato non è in grado di ottenerne una copia dal cliente.

5.5. Responsabilità. Glarish sarà responsabile per gli atti e le omissioni dei suoi Subincaricati non affiliati nella stessa misura in cui Glarish sarebbe responsabile, se prestasse i servizi di ciascun responsabile direttamente secondo i termini di questo DPA.

6. LUOGHI DELLE STRUTTURE

Le parti convengono che il Software, incluso il Portale, e tutti i Dati personali, inclusi i relativi backup, saranno ospitati e / o archiviati presso strutture situate nei data center nell'UE e / o negli Stati Uniti. Se Glarish propone di ospitare o archiviare il Software, incluso il Portale, o i backup, e qualsiasi Dato personale, presso strutture situate al di fuori degli Stati Uniti o dello Spazio economico europeo ("Struttura straniera"), Glarish fornirà una comunicazione scritta preventiva al Cliente fornendo i dettagli di tale proposta ("Avviso di ricollocazione"). Il Cliente può, a sua esclusiva discrezione, opporsi alla proposta di Struttura Estera. Se le parti non riescono a concordare una risoluzione entro sessanta (60) giorni dall'obiezione del Cliente, il Cliente può risolvere il presente Contratto. Glarish non consentirà al Software, incluso il Portale, o ai backup del Software, né ai Dati personali, di essere ospitati e / o archiviati da una struttura estera a meno che e fino a quando non sia stato concordato per iscritto dal Cliente.

7. SECURITY

Tenendo conto dello stato dell'arte, dei costi di implementazione e della natura, portata, contesto e finalità del Trattamento, nonché del rischio di variazione della probabilità e della gravità per i diritti e le libertà delle persone fisiche, Glarish deve implementare adeguate procedure organizzative e tecniche misure per garantire un livello di sicurezza adeguato al rischio (inclusa la protezione da distruzione accidentale o illegale, alterazione della perdita, divulgazione non autorizzata o accesso ai Dati personali elaborati ai sensi del presente DPA), come stabilito nell'Allegato 2 a questo DPA. Glarish deve monitorare regolarmente il rispetto di queste misure. Glarish non diminuirà materialmente la sicurezza complessiva dei Servizi durante il periodo di abbonamento del Cliente. L'Allegato 2 può essere modificato di volta in volta, previo accordo scritto delle parti, per soddisfare standard più elevati di sicurezza e privacy. In tal caso, l'appendice 2 deve essere sostituito. Il Cliente dichiara che, dopo la sua valutazione dei requisiti delle leggi e dei regolamenti sulla protezione dei dati, il Cliente ritiene che le misure di sicurezza stabilite nell'Allegato 2 siano appropriate per proteggere i Dati personali da distruzione accidentale o illegale o perdita accidentale, alterazione, divulgazione o accesso non autorizzati, e contro tutte le altre forme illecite di Trattamento, e che queste misure garantiscano un livello di sicurezza adeguato ai rischi presentati dal Trattamento e alla natura dei Dati Personali da proteggere tenendo conto dello stato dell'arte e del costo della loro attuazione.

8. VIOLAZIONI DI DATI PERSONALI (DATA BREACH) E NOTIFICHE

Glarish ha in atto politiche e procedure di gestione degli incidenti di sicurezza ragionevoli e appropriate, specificate nell'Allegato 2 di questo DPA, e informerà il Cliente senza ingiustificato ritardo dopo essere venuto a conoscenza di una distruzione, alterazione o danno o perdita illegale o accidentale, divulgazione non autorizzata o l'accesso ai Dati personali, trasmessi, archiviati o altrimenti elaborati da Glarish o dai suoi Subincaricati non affiliati di cui Glarish viene a conoscenza

("Violazioni di dati personali"), come richiesto dall'articolo 33 del GDPR. Glarish compirà ogni ragionevole sforzo per identificare la causa di tale violazione dei dati personali e intraprenderà le misure che ritiene necessarie e ragionevoli al fine di porre rimedio alla causa di tale violazione dei dati personali, nella misura in cui la riparazione sia sotto il ragionevole controllo di Glarish.

9. CERTIFICAZIONE E AUDIT

9.1 Audit. Su richiesta del Cliente e soggetta alla riservatezza stabilita nel Contratto, Glarish metterà a disposizione del Cliente che non è un concorrente di Glarish tutte le informazioni necessarie per dimostrare la conformità con gli obblighi di Glarish ai sensi del presente DPA, e consentirà e contribuirà all'audit, anche in loco, condotti dal Cliente o da un revisore indipendente di terza parte del Cliente, in possesso delle qualifiche professionali richieste vincolate da un obbligo di riservatezza, che non sia concorrente di Glarish. Le parti convengono che gli audit siano effettuati in conformità con le seguenti specifiche: Il cliente può contattare Glarish per richiedere un audit in loco dell'architettura, dei sistemi e delle procedure rilevanti per la protezione dei dati personali. Il Cliente rimborserà Glarish per qualsiasi tempo speso da Glarish o dai suoi sub-processori di terze parti per qualsiasi verifica in loco in base alle tariffe dei servizi professionali di Glarish in quel momento, che saranno messe a disposizione del Cliente su richiesta. Prima dell'inizio di tale verifica in loco, il Cliente e Glarish concorderanno reciprocamente l'ambito, la tempistica e la durata della verifica oltre al tasso di rimborso di cui il Cliente sarà responsabile. Tutti i tassi di rimborso devono essere ragionevoli, tenendo conto delle risorse spese da Glarish o dai suoi sub-processori di terze parti. Il Cliente dovrà informare tempestivamente Glarish e fornire informazioni su qualsiasi non conformità effettiva o sospetta rilevata durante un audit.

9.2 Certificazioni. Glarish dovrà inoltre consentire e fornire certificazioni di terze parti e risultati di audit su richiesta scritta del Cliente a intervalli ragionevoli e soggetti agli obblighi di riservatezza stabiliti nel Contratto. Glarish metterà a disposizione del Cliente che non è un concorrente di Glarish

(il revisore indipendente di terze parti del Cliente che non è un concorrente di Glarish) una copia delle certificazioni di terze parti o dei risultati di audit più recenti di Glarish, a seconda dei casi.

10. REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO E COLLABORAZIONE CON L'AUTORITÀ DI CONTROLLO (GARANTE PRIVACY)

10.1. Registri. Ove applicabile, Glarish manterrà una registrazione, in formato elettronico, di tutte le categorie di attività di trattamento svolte per conto del Cliente, ai sensi dell'articolo 30, paragrafo 2, GDPR.

10.2. Collaborazione con l'Autorità di Vigilanza. Ove applicabile, Glarish, su richiesta, collabora con l'autorità di controllo (garante privacy) nello svolgimento dei propri compiti, di cui all'art. 31 del GDPR.

11. RESTITUZIONE E CANCELLAZIONE DEI DATI PERSONALI

Glarish dovrà, a scelta del Cliente, restituire i Dati Personali al Cliente o cancellare le copie esistenti dopo la fine della fornitura dei Servizi e certificare al Cliente di averlo fatto in conformità con le procedure specificate nell'Allegato 2 al presente DPA, a meno che le leggi obbligatorie non richiedano l'archiviazione dei dati personali. In tal caso Glarish assicura che garantirà la riservatezza dei Dati personali e non elaborerà più attivamente i Dati personali trasferiti.

12. VALUTAZIONE DELL'IMPATTO SULLA PROTEZIONE DEI DATI

Su richiesta del Cliente, Glarish fornirà al Cliente la ragionevole cooperazione e assistenza necessarie per adempiere all'obbligo del Cliente ai sensi dell'articolo 35 del GDPR di eseguire una Valutazione dell'impatto sulla protezione dei dati ("DPIA") relativa all'uso dei Servizi da parte del Cliente, nella misura in cui il Cliente lo fa non avere altrimenti accesso alle informazioni pertinenti e nella misura in cui tali informazioni siano disponibili per Glarish. Glarish fornirà ragionevole assistenza al Cliente

nella cooperazione o previa consultazione con l'Autorità di controllo nello svolgimento dei suoi compiti relativi al presente DPA, nella misura richiesta dall'articolo 36 del GDPR.

13. TRASFERIMENTO DEI DATI

i. I trasferimenti di dati personali ai sensi del presente DPA dall'Unione Europea, dallo Spazio economico europeo e / o dai loro stati membri, dalla Svizzera e dal Regno Unito verso paesi al di fuori dello Spazio economico europeo sono effettuati solo in conformità con quanto segue:

ii. il trasferimento avviene verso una giurisdizione per la quale è stata emessa una decisione di adeguatezza e soggetta ai termini di tale decisione di adeguatezza;

iii. in assenza di una Decisione di Adeguatezza, il trasferimento è soggetto alle ultime versioni delle Clausole Contrattuali Standard approvate di volta in volta dalla Commissione Europea, così come pubblicate nella Gazzetta Ufficiale dell'Unione Europea, e che a loro volta fanno parte del presente DPA (Allegato 4).

14. AFFILIATI AUTORIZZATI

14.1 Rapporto contrattuale. Le parti riconoscono e concordano che, eseguendo il DPA, il Cliente entra nel DPA per conto proprio e, se applicabile, in nome e per conto dei suoi Affiliati autorizzati, stabilendo così un DPA separato tra Glarish e ciascuno tale Affiliato Autorizzato soggetto alle disposizioni dell'Accordo e della presente Clausola e della Clausola 15 di questo DPA. Ogni Affiliato Autorizzato accetta di essere vincolato dagli obblighi ai sensi del presente DPA e, nella misura applicabile, del Contratto. A scanso di equivoci, un Affiliato Autorizzato non è e non diventa una parte dell'Accordo ed è solo una parte dell'Accordo. Tutti gli accessi e l'utilizzo dei Servizi e dei Contenuti da parte degli Affiliati autorizzati devono essere conformi ai termini e alle condizioni dell'Accordo e qualsiasi violazione dei

termini e delle condizioni dell'Accordo da parte di un Affiliato autorizzato sarà considerata una violazione del Cliente.

14.2 Comunicazione. Il Cliente che è parte contraente dell'Accordo rimarrà responsabile del coordinamento di tutte le comunicazioni con Glarish ai sensi del presente DPA e avrà il diritto di effettuare e ricevere qualsiasi comunicazione in relazione a questo DPA per conto dei suoi Affiliati autorizzati. Il Cliente informa Glarish degli Affiliati Autorizzati ai quali il Cliente intende consentire l'utilizzo dei Servizi, dando così a Glarish l'opportunità di opporsi, nel caso in cui i requisiti stabiliti nella Definizione di Affiliato Autorizzato ai sensi del presente DPA non siano soddisfatti.

14.3 Diritti degli affiliati autorizzati. Laddove un Affiliato autorizzato diventa parte del DPA con Glarish, nella misura richiesta dalle leggi e dai regolamenti applicabili sulla protezione dei dati, avrà il diritto di esercitare i diritti e cercare rimedi ai sensi del presente DPA, fatto salvo quanto segue:

i. Ad eccezione dei casi in cui le leggi e i regolamenti applicabili in materia di protezione dei dati richiedono all'Affiliato Autorizzato di esercitare un diritto o di cercare qualsiasi rimedio ai sensi del presente DPA contro Glarish direttamente da solo, le parti concordano che (a) esclusivamente il Cliente che è la parte contraente del Contratto tale diritto o cercare qualsiasi rimedio per conto dell'Affiliato Autorizzato, e (b) il Cliente che è la parte contraente dell'Accordo eserciterà tali diritti ai sensi del presente DPA non separatamente per ogni Affiliato Autorizzato individualmente ma in modo combinato per tutti delle sue Affiliate Autorizzate insieme (come stabilito, ad esempio, nella Sezione 13.3.ii di seguito).

ii. Le parti convengono che il Cliente che è la parte contraente dell'Accordo, quando esegue una verifica in loco sulle procedure relative alla protezione dei Dati personali, adotta tutte le misure ragionevoli per limitare qualsiasi impatto su Glarish e sui suoi non affiliati Subincaricati combinando, per quanto ragionevolmente possibile, diverse richieste di audit eseguite per conto di diverse Affiliate Autorizzate in un unico audit.

15. RESPONSABILITÀ

A scanso di equivoci, la responsabilità totale di Glarish per tutti i reclami del Cliente e di tutte le sue affiliate autorizzate derivanti da o correlati al Contratto e ogni DPA si applicherà in forma aggregata per tutti i reclami ai sensi del Contratto e di tutti i DPA stabiliti ai sensi del presente Contratto, incluso da parte del Cliente e di tutte le affiliate autorizzate, e in particolare, non deve essere inteso come applicabile individualmente e separatamente al Cliente e / o a qualsiasi Affiliato autorizzato che è parte contrattuale di tali DPA.

16. EFFETTI LEGALI; TERMINAZIONE; VARIAZIONE

Questo DPA diventerà legalmente vincolante tra il Cliente e Glarish solo quando sarà completamente eseguito seguendo i passaggi delle formalità indicati nella Sezione "Come eseguire questo DPA" e terminerà quando l'Accordo principale terminerà, senza ulteriori azioni richieste da nessuna delle parti. Le parti si impegnano a non variare o modificare il DPA. Ciò non preclude alle parti di aggiungere clausole su questioni relative alle imprese, ove richiesto purché non siano in contraddizione con il DPA.

17. CONFLITTI

Questo DPA è incorporato e fa parte dell'Accordo. Per questioni non trattate in questo DPA, si applicano i termini del Contratto. Per quanto riguarda i diritti e gli obblighi delle parti l'una nei confronti dell'altra, in caso di conflitto tra i termini dell'Accordo e questo DPA, prevarranno i termini di questo DPA. IN FEDE, le parti hanno operato affinché la presente Allegato sulla Protezione dei dati fosse debitamente eseguita. Ciascuna parte garantisce e dichiara che i suoi rispettivi firmatari, le cui firme sono riportate di seguito, sono alla data della firma debitamente autorizzati.

CLIENTE GLARISH

ALLEGATO 1

Detttaglio del Trattamento dei Dai

Questo allegato include alcuni dettagli sul Protezione dei dati personali come richiesto dall'articolo 28, paragrafo 3, del GDPR.

Finalità del Trattamento dei Dati

Glarish elaborerà i Dati personali come necessario per eseguire i Servizi ai sensi del Contratto e come ulteriormente indicato dal Cliente nell'utilizzo dei Servizi.

Durata del Trattamento dei Dati

Fatta salva la clausola 11 del DPA, Glarish elaborerà i dati personali per la durata del contratto, salvo diverso accordo scritto. Salvo diverso accordo scritto, Glarish, a scelta del Cliente, restituirà i Dati personali al Cliente o cancellerà le copie esistenti dopo la fine della fornitura dei Servizi e certificherà al Cliente di averlo fatto in conformità con il procedure specificate nell'Allegato 2 al presente DPA, a meno che leggi imperative non richiedano la conservazione dei Dati personali. In tal caso Glarish garantisce che garantirà la riservatezza dei Dati personali e non elaborerà più attivamente i Dati personali trasferiti.

Categorie dei Dati Soggetti a Trattamento

• Clienti

• Agenti dei Clienti, Dipendenti, Utenti Autorizzati

Tipo di Dati Personali

• Dati di identificazione:

- nome, indirizzo, email, numero di telefono e diritti di accesso.

• Contenuto del cliente:

- Immagini
- Video
- Power point
- File Pdf ecc

ATTACHMENT 2

Descrizione delle misure di sicurezza tecniche e organizzative implementate da Glarish ai sensi dell'articolo 28.3 del GDPR, che fanno parte del DPA:

- **Personale Addetto**

Riservatezza e affidabilità. Il personale addetto al Protezione dei dati personali è affidabile, è informato della natura riservata dei Dati personali, ha ricevuto una formazione adeguata sulle proprie responsabilità, è regolarmente formato e ha sottoscritto accordi di riservatezza scritti. Gli obblighi di riservatezza sopravvivono alla cessazione dell'impegno del personale. I privilegi di accesso cessano alla cessazione del rapporto di lavoro. Tutto il personale con diritto di accesso agli Account è assunto a tempo pieno.

Separazione dei doveri e limitazione dell'accesso. *L'accesso del personale ai dati personali è appropriato e necessario per il suo ruolo. Un responsabile della sicurezza è stato nominato per iscritto e controlla il rispetto delle misure di sicurezza. Il personale dispone di account individuali per l'accesso ai sistemi con codici di sicurezza. Il personale è suddiviso in tre livelli di accesso i) sviluppatori, ii) supporto / vendita e iii) altri. Gli sviluppatori hanno accesso all'intero sistema, per garantire che tutto funzioni senza problemi. Il supporto ha un accesso limitato al sistema, cioè solo quando si gestisce una richiesta di supporto. Tutti gli altri non hanno accesso agli account.*

Controllo degli accessi e autenticazione. *È in atto una procedura per la creazione e l'eliminazione dell'account utente, con le approvazioni appropriate; b. Vengono utilizzate pratiche standard del settore per identificare e autenticare gli utenti che tentano di accedere ai sistemi di informazione; c. Gli identificatori disattivati o scaduti non vengono concessi ad altri individui; d. Tutte le azioni del personale vengono registrate in un registro di controllo interno. Fornire supporto appare anche agli utenti di un account, se l'account è nel piano Enterprise che prevede le funzionalità "log di controllo".*

- **Sistemi e Metodologie e Strutture di Sicurezza**

Accesso fisico*. Glarish utilizza strutture con controllo degli accessi (ad esempio CCTV, sistemi di sicurezza intelligenti, reception, codice di accesso) e con piani di emergenza e di emergenza per vari disastri, incluso l'incendio. Le esercitazioni vengono praticate regolarmente.*

Esposizione di documenti. *Viene implementata una politica di "Scrivanie Pulite". Tutti i documenti (file) fisici sono conservati in armadi o cassetti. Fotocopiatrici e fax non sono in vista comune.*

Distruzione di documenti. *Le carte con dati personali vengono distribuite esclusivamente nei trituratori di carta. Dopo il periodo di conservazione, i dati elettronici non vengono solo cancellati, ma distrutti (inclusi i relativi backup) sovrascrivendoli con l'uso di software speciali, come cancellatori di file, trituratori di file, polverizzatori di file o, in alternativa, per la distruzione su base giornaliera, da formattazione.*

Dispositivi portatili. *I laptop sono accessibili solo tramite codici protetti.*

- **SICUREZZA DEI DATI**

Antivirus. *Glarish garantisce l'installazione di software antivirus, anti-malware e anti-spyware dell'ultimo aggiornamento. Gli aggiornamenti vengono installati a intervalli regolari. Glarish intraprende attività di protezione avanzata, per ridurre al minimo i punti deboli dell'architettura dei sistemi operativi, delle applicazioni e dei dispositivi di rete.*

Accesso remoto. *La sicurezza dell'accesso remoto al sistema si basa sulla crittografia e su protocolli sicuri. È consentita solo la comunicazione diretta tra il dispositivo e il server, non è consentito l'inoltro del traffico o il traffico tra i dispositivi.*

Firewall*. Viene installato un firewall standard del settore per ispezionare tutte le connessioni instradate all'ambiente del sistema.*

Test di vulnerabilità e penetrazione. *Glarish esegue periodicamente analisi di vulnerabilità finalizzate a specificare lo stato di esposizione a vulnerabilità note, in relazione sia agli ambienti infrastrutturali che applicativi, considerando i sistemi in esercizio o in fase di sviluppo. Tali verifiche avvengono periodicamente, semestralmente, integrate da specifici test di penetrazione, comportando simulazioni di intrusione che utilizzano differenti scenari di attacco.*

Controllo delle modifiche. *Tutte le modifiche alla piattaforma, all'applicazione e all'infrastruttura di produzione (ad esempio aggiornamento del software, sviluppo di nuovo software, installazione o disinstallazione di antivirus) vengono testate, prima dell'implementazione, in un ambiente isolato e aggiornato che non influisce sui dati reali o sui dati del sistema di produzione, ad eccezione degli utenti che si sono iscritti alla Beta Set Up. Ci sono controlli regolari sul software installato per verificare che nessun software sia stato installato al di fuori del normale processo. Tutte le modifiche vengono gestite centralmente solo da utenti specifici.*

Separazione dei dati. *Il contenuto caricato nel software GLARISH deve essere mantenuto logicamente separato dall'infrastruttura aziendale di Glarish e dai contenuti degli altri clienti di Glarish.*

- **Registrazione Accessi (Log management)**

Generale. *I log sono delle registrazioni sequenziali e cronologiche delle operazioni effettuate da un sistema informatico. I file di registro vengono conservati per tutti i sistemi cruciali. Glarish conserva i seguenti tipi di log: Log di accesso al Web / Log dell'applicazione / Log di controllo (dettagliati). Le seguenti informazioni sono necessariamente conservate come minimo:*

a) identificazione dell'utente che ha richiesto l'accesso ai dati personali, data e ora della richiesta, sistema per il quale è stato richiesto l'accesso, se l'accesso è stato concesso o meno.

b) Stesse informazioni per quanto riguarda gli accessi non autorizzati

c) Stampa richieste di file con dati personali

d) Modifiche nei file cruciali del sistema o nei diritti degli utenti

e) Modifiche ai parametri di app e sistemi

f) Eventi cruciali e di qualsiasi azione che possa essere considerata un attacco o un incidente di sicurezza (ad es. scansione delle porte). La conservazione degli eventi è supervisionata direttamente dal Security Officer e dagli Amministratori di Sistema.

I file di registro possono essere valutati solo dal responsabile della sicurezza e dagli amministratori di sistema. L'eliminazione dei file di registro deve essere autorizzata sia dal responsabile della sicurezza che da un membro dell'alta dirigenza.

Memorizzazione dei Log. Tutti i log vengono caricati da ogni server su Google Cloud. Le credenziali e i nomi utilizzati garantiscono che un utente malintenzionato non possa accedere o alterare i registri. Glarish utilizza il controllo delle versioni su Google Cloud per assicurarsi che i contenuti precedenti dei log aggiornati vengano conservati. I file di registro vengono archiviati in un bucket Google Cloud adeguatamente configurato per la crittografia dei dati inattivi utilizzando lo schema di crittografia di Google.

Rotazione dei Log. Tutti i log vengono ruotati sul server su base di 5 giorni, per facilitare il supporto e il debug. I registri archiviati su Google Cloud vengono ruotati ogni 90 giorni.

- **Password**

L'accesso a tutti i sistemi, applicazioni e software è protetto da password. Le password ammissibili sono conformi alle configurazioni delle password (es. Lunghezza minima, scadenza, complessità, ecc.). La modifica delle password viene applicata regolarmente.

Le password non vengono scritte, né fisicamente né elettronicamente, nella loro forma effettiva. Sono conservati elettronicamente in una forma non leggibile, mentre è possibile il recupero della loro forma iniziale. Dopo tre tentativi di autorizzazione di accesso non riusciti, l'accesso è vietato all'utente.

Le password non vengono conservate nei registri.

Vengono implementate procedure standard di settore per disattivare le password che sono state danneggiate o divulgate inavvertitamente.

- **Sistemi di Continuità and Recupero Disastri (Disaster Recovery)**

Glarish utilizza strutture (data center), per i dati personali e il loro backup, fornendo adeguati piani e garanzie di emergenza e di emergenza; b. Glarish dispone di adeguate procedure di recupero dei dati.

- **Monitoraggio e Gestione degli Incidenti**

Glarish monitora, analizza e risponde agli incidenti di sicurezza in modo tempestivo e si intensifica secondo necessità. Glarish implementa una specifica Procedura di Incident Management per garantire il ripristino delle normali operazioni di servizio il prima possibile in caso di interruzione.

- **Gestione del Data Breach**

Glarish ha in atto una politica sulla violazione dei dati per soddisfare i requisiti della clausola 8 di questo DPA e del GDPR, che include ma non è limitata a i) la segnalazione interna di potenziali violazioni dei dati personali, ii) il recupero di una violazione dei dati personali, iii) valutazione del rischio, iv) notifica di violazione dei dati personali al titolare del trattamento, all'autorità di controllo e all'interessato, se applicabile, v) misure di valutazione e risposta per prevenire violazioni simili. Il responsabile della sicurezza è responsabile dell'implementazione e dell'aggiornamento della politica sulla violazione dei dati.

- **Progettazione dei Servizi**

Privacy. Ogni utente, dopo essersi registrato per la prima volta, deve accettare l'Informativa sulla privacy di Glarish. L'applicazione GLARISH consente al Cliente di assegnare diritti specifici (di visualizzazione, accesso, modifica ed eliminazione) in base ai compiti e alle responsabilità dell'Affiliato Autorizzato o dell'Utente Autorizzato. La cancellazione dei dati personali così come la cancellazione dell'account è possibile tramite il processo descritto nella dashboard nella sezione "Dati personali". Sono previste le seguenti misure di sicurezza: a) autenticazione degli utenti prima dell'accesso; ii) crittografia delle password iii) attivazione della policy per la password sicura da parte del cliente nel piano aziendale; iv) cambio di password ogni sei mesi; e iv) prevenzione dell'accesso dopo tentativi di accesso sospetti.

Responsabilità dei Clienti. Il Cliente gestisce l'accesso di ogni utente e l'utilizzo dei Servizi assegnando a ciascun utente una credenziale e un tipo di utente che controlla il livello di accesso e utilizzo dei Servizi. Il Cliente è responsabile della protezione della riservatezza del proprio login e della password di ogni utente e della gestione dell'accesso di ciascun utente ai Servizi.

Sicurezza. Traffico in uscita sicuro. L'applicativo GLARISH non utilizza la porta di ascolto UDP (UDP). L'applicativo GLARISH non utilizza il port forwarding, DMZ o UPnP nella rete. L'applicazione Glarish utilizza canali di comunicazione full-duplex su una singola connessione TCP tramite una crittografia TLS / SSL per crittografare tutti i dati inviati da e verso il server (inclusi l'handshake e la risposta iniziali), che è lo stesso meccanismo di crittografia utilizzato per le connessioni HTTPS (e utilizza lo stesso motore di crittografia nel browser).

Digital Signature e Verifica del Software. Glarish ha sviluppato un protocollo proprietario che non consente a un utente malintenzionato di forzare il lettore multimediale a riprodurre un file di pianificazione diverso da quello generato dal sistema per questo dispositivo specifico. Due motivi:

(1) il media player non contiene informazioni sul software di base quando è disconnesso dal server certificato; (2) il software di base è strettamente associato al numero di serie della scheda.

HTTPS Certificate checks. File di pianificazione, file di configurazione e file multimediali vengono scaricati utilizzando HTTPS. Il controllo del certificato SSL viene applicato in tutto il sistema.

Aggiornamento del Software e Sistemi di Controllo. Glarish adotta un aggiornamento virtuale del software attraverso una tecnologia proprietaria che assicura gli ultimi aggiornamenti software in qualsiasi momento. Il software viene scaricato tramite HTTPS.

Firewall dei Dispositivi. I dispositivi GLARISH hanno una policy firewall standard abilitata per impostazione predefinita, che consente solo l'accesso SSH in entrata. SSH può anche essere un firewall per l'interfaccia LAN, senza lasciare nulla accessibile dalla LAN, senza alcuna interruzione del servizio.

Autenticazione Supporti Proxy. I dispositivi GLARISH supportano l'utilizzo di un proxy installato e gestito. Il proxy è necessario per supportare il metodo "CONNECT" per le connessioni HTTPS. Glarish supporta l'utilizzo delle credenziali di autenticazione per i proxy.

Codice di Personalizzazione. I codici di personalizzazione del supporto del dispositivo per modificare il comportamento predefinito vengono emessi in remoto come parte del file di configurazione, che è firmato digitalmente e protetto.

Inizializzazione Sicura del Software. La scheda SD che contiene il software Player deve essere scritta tramite un altro computer come immagine disco. Un utente registrato può scaricare l'immagine della scheda SD. La scheda SD può essere inserita nello slot per scheda SD del lettore multimediale.

Connessione USB disabilitata per sicurezza. Tutti i connettori USB sono completamente disabilitati. Il media player può funzionare solo tramite Internet.

Protezione del Media Player da attacchi di hackers. Qualsiasi modifica esterna (hacking) del software nella scheda SD comprometterebbe l'auto-inizializzazione sicura del media player e disabiliterebbe la connessione con il server.

Customer's responsibility. Il cliente è l'unico responsabile per la connessione sicura del lettore GLARISH a Internet.

- **Audit e Revisione**

L'audit interno ed esterno di tutti i sistemi avviene su base semestrale. Le misure di sicurezza tecnica e organizzativa vengono riviste annualmente e in caso di modifiche importanti. L'audit e la revisione includono la pianificazione della capacità delle risorse IT in vista dei requisiti futuri in base al carico di lavoro e ai requisiti di archiviazione dei dati.

ATTACHMENT 3

L'elenco dei Subincaricati non Affiliati approvati dal Cliente alla data di entrata in vigore del DPA è come stabilito di seguito;

Responsabile non affiliato Descrizione del trattamento Informazioni di contatto Posizione delle strutture (incluso il backup)

Fornitori

Google Cloud www.google.com USA

Stripe Payments www.stripe.com USA

ATTACHMENT 4

DECISIONE DELLA COMMISSIONE

del 5 febbraio 2010

relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio

[notificata con il numero C(2010) 593]

(Testo rilevante ai fini del SEE)

(2010/87/UE)

ALLEGATO CLAUSOLE CONTRATTUALI TIPO («INCARICATI DEL TRATTAMENTO») Ai sensi dell'articolo 26, paragrafo 2, della direttiva 95/46/CE per il trasferimento di dati personali a subincaricati del trattamento stabiliti in paesi terzi che non garantiscono un livello adeguato di protezione dei dati Nome dell'organizzazione esportatrice:

.....

Indirizzo:

.....

..... Tel. .....;Fax

.....; E-mail: ..... Altre informazioni identificative:

.....

..... («l'esportatore») e Nome dell'organizzazione importatrice:

.....

Indirizzo:

.....

..... Tel. .....;Fax

.....; E-mail: ..... Altre informazioni identificative:

.....

..... («l'importatore») denominato ciascuno «parte» e congiuntamente «parti», HANNO CONVENUTO le seguenti clausole contrattuali («le clausole») al fine di prestare garanzie sufficienti con riguardo alla tutela della vita privata e dei diritti e delle libertà fondamentali delle persone per il trasferimento dall'esportatore all'importatore dei dati personali indicati nell'appendice 1

Clausola 1

Definizioni

Ai fini delle presenti clausole:

a) I termini «dati personali», «categorie particolari di dati», «trattamento», «responsabile del trattamento», «incaricato del trattamento», «interessato/persona interessata» e «autorità di controllo» hanno la stessa accezione attribuita nella direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al Protezione dei dati personali, nonché alla libera circolazione di tali dati ([1]);

b) con «esportatore» s'intende il responsabile del trattamento che trasferisce i dati personali;

c) con «importatore» s'intende l'incaricato del trattamento stabilito in un paese terzo che s'impegni a ricevere dall'esportatore dati personali al fine di trattarli per conto e secondo le istruzioni dell'esportatore stesso, nonché a norma delle presenti clausole, e che non sia assoggettato dal paese terzo a un sistema che garantisca una protezione adeguata ai sensi dell'articolo 25, paragrafo 1, della direttiva 95/46/CE;

d) con «terzo incaricato» s'intende l'incaricato del trattamento designato dall'importatore o da altro suo terzo incaricato, che s'impegni a ricevere dall'importatore o da altro suo terzo incaricato dati personali al solo fine di trattarli per conto e secondo le istruzioni dell'esportatore, nonché a norma delle presenti clausole e del subcontratto scritto;

e) con «normativa sulla protezione dei dati» si intende la normativa che protegge i diritti e le libertà fondamentali del singolo, in particolare il diritto al rispetto della vita privata con riguardo al trattamento di dati personali, applicabile ai subincaricati del trattamento nello Stato membro in cui è stabilito l'esportatore;

f) con «misure tecniche e organizzative di sicurezza» s'intendono le misure destinate a garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali.

Clausola 2

Particolari del trasferimento

I particolari del trasferimento, segnatamente le categorie particolari di dati personali, sono indicati nell'appendice 1 che costituisce parte integrante delle presenti clausole.

Clausola 3

Clausola del terzo beneficiario

1. L'interessato può far valere, nei confronti dell'esportatore, la presente clausola, la clausola 4, lettere da b) a i), la clausola 5, lettere da a) ad e) e da g) a j), la clausola 6, paragrafi 1 e 2, la clausola 7, la clausola 8, paragrafo 2, e le clausole da 9 a 12 in qualità di terzo beneficiario.

2. L'interessato può far valere, nei confronti dell'importatore, la presente clausola, la clausola 5, lettere da a) ad e) e g), la clausola 6, la clausola 7, la clausola 8, paragrafo 2, e le clausole da 9 a 12 qualora l'esportatore sia scomparso di fatto o abbia giuridicamente cessato di esistere, a meno che tutti gli obblighi dell'esportatore siano stati trasferiti, per contratto o per legge,

all'eventuale successore che di conseguenza assume i diritti e gli obblighi dell'esportatore, nel qual caso l'interessato può far valere le suddette clausole nei confronti del successore.

3. L'interessato può far valere, nei confronti del terzo incaricato, la presente clausola, la clausola 5, lettere da a) ad e) e g), la clausola 6, la clausola 7, la clausola 8, paragrafo 2, e le clausole da 9 a 12 qualora sia l'esportatore che l'importatore siano scomparsi di fatto, abbiano giuridicamente cessato di esistere o siano divenuti insolventi, a meno che tutti gli obblighi dell'esportatore siano stati trasferiti, per contratto o per legge, all'eventuale successore che di conseguenza assume
i diritti e gli obblighi dell'esportatore, nel qual caso l'interessato può far valere le suddette clausole nei confronti del successore. La responsabilità civile del terzo incaricato è limitata ai trattamenti da quello effettuati ai sensi delle presenti clausole.

4. Le parti non si oppongono a che l'interessato sia rappresentato da un'associazione o altra organizzazione, ove siffatta rappresentanza corrisponda alla esplicita volontà dell'interessato e sia ammessa dalla legislazione nazionale.

Clausola 4

Obblighi dell'esportatore

L'esportatore dichiara e garantisce quanto segue:

a) che il trattamento, compreso il trasferimento, dei dati personali, è e continua ad essere effettuato in conformità di tutte le pertinenti disposizioni della normativa sulla protezione dei dati (e viene comunicato, se del caso, alle competenti autorità dello Stato membro in cui è stabilito l'esportatore) nel pieno rispetto delle leggi vigenti in quello Stato;

b) che ha prescritto all'importatore, e continuerà a farlo per tutta la durata delle operazioni di trattamento, di trattare i dati personali trasferiti soltanto per suo conto e conformemente alla normativa sulla protezione dei dati e alle presenti clausole;

c) che l'importatore fornirà sufficienti garanzie per quanto riguarda le misure tecniche e organizzative di sicurezza indicate nell'appendice 2;

d) che, alla luce della normativa sulla protezione dei dati, le misure di sicurezza sono atte a garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali, e che tali misure garantiscono un livello di sicurezza commisurato ai rischi inerenti al trattamento e alla natura dei dati da tutelare, tenuto conto della più recente tecnologia e dei costi di attuazione;

e) che provvederà all'osservanza delle misure di sicurezza;

f) che, qualora il trasferimento riguardi categorie particolari di dati, gli interessati sono stati o saranno informati prima del trasferimento, o immediatamente dopo, che i dati che li riguardano potrebbero essere trasmessi a un paese terzo che non garantisce una protezione adeguata ai sensi della direttiva 95/46/CE;

g) di trasmettere all'autorità di controllo l'eventuale comunicazione presentata dall'importatore o dal terzo incaricato ai sensi della clausola 5, lettera b), e della clausola 8, paragrafo 3, qualora decida di proseguire il trasferimento o revocare la sospensione;

h) che fornirà, su richiesta degli interessati, copia delle presenti clausole, esclusa l'appendice 2, e una descrizione generale delle misure di sicurezza, nonché copia dei subcontratti aventi ad oggetto il trattamento da effettuarsi in conformità delle presenti clausole, omettendo le informazioni commerciali eventualmente contenute nelle clausole o nel contratto;

i) che, in caso di subcontratto, il terzo incaricato svolge l'attività di trattamento in conformità della clausola 11 garantendo un livello di protezione dei dati personali e dei diritti dell'interessato quanto meno uguale a quello cui è tenuto l'importatore ai sensi delle presenti clausole;

j) che provvederà all'osservanza della clausola 4, lettere da a) ad i).

Clausola 5

Obblighi dell'importatore ([1])

L'importatore dichiara e garantisce quanto segue:

a) di trattare i dati personali esclusivamente per conto e secondo le istruzioni dell'esportatore, nonché a norma delle presenti clausole, e di impegnarsi a informare prontamente l'esportatore qualora non possa per qualsiasi ragione ottemperare a tale disposizione, nel qual caso l'esportatore ha facoltà di sospendere il trasferimento e/o risolvere il contratto;

b) di non avere motivo di ritenere che la normativa ad esso applicabile impedisca di seguire le istruzioni dell'esportatore o di adempiere agli obblighi contrattuali, e di comunicare all'esportatore, non appena ne abbia conoscenza, qualsiasi modificazione di tale normativa che possa pregiudicare le garanzie e gli obblighi previsti dalle presenti clausole, nel qual caso l'esportatore ha facoltà di sospendere il trasferimento e/o di risolvere il contratto;

c) di aver applicato le misure tecniche e organizzative di sicurezza indicate nell'appendice 2 prima di procedere al Protezione dei dati personali trasferiti;

([1]) Disposizioni vincolanti della legislazione nazionale applicabile all'importatore che non vanno oltre quanto è necessario in una società democratica sulla base di uno degli interessi di cui all'articolo 13, paragrafo 1, della direttiva 95/46/CE; in altri termini, le restrizioni necessarie alla salvaguardia della sicurezza dello Stato, della difesa, della pubblica sicurezza, della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate, di un rilevante interesse economico o finanziario dello Stato, della protezione della persona cui si riferiscono i dati o dei diritti o delle libertà altrui, non sono in contraddizione con le clausole contrattuali tipo. Costituiscono esempi di disposizioni vincolanti che non vanno oltre quanto è necessario in una società democratica le sanzioni internazionalmente riconosciute, gli obblighi di informazione in materia fiscale o contro il riciclaggio di capitali.

d) che comunicherà prontamente all'esportatore:

i) qualsiasi richiesta giuridicamente vincolante presentata da autorità giudiziarie o di polizia ai fini della comunicazione di dati personali, salvo che la comunicazione sia vietata da norme specifiche, ad esempio da norme di diritto penale miranti a tutelare il segreto delle indagini;

ii) qualsiasi accesso accidentale o non autorizzato; e

iii) qualsiasi richiesta ricevuta direttamente dagli interessati cui non abbia risposto, salvo che sia stato autorizzato a non rispondere;

e) che risponderà prontamente e adeguatamente a tutte le richieste dell'esportatore relative al Protezione dei dati personali soggetti a trasferimento e che si conformerà al parere dell'autorità di controllo per quanto riguarda il Protezione dei dati trasferiti;

f) che sottoporrà i propri impianti di trattamento, su richiesta dell'esportatore, al controllo dell'esportatore o di un organismo ispettivo composto da soggetti indipendenti, in possesso delle necessarie qualificazioni professionali, vincolati da obbligo di riservatezza e selezionati dall'esportatore, eventualmente di concerto con l'autorità di controllo;

g) che fornirà, su richiesta degli interessati, copia delle presenti, esclusa l'appendice 2, e una descrizione generale delle misure di sicurezza qualora gli interessati non siano in grado di ottenerne copia direttamente dall'esportatore, o copia dei subcontratti del trattamento, omettendo le informazioni commerciali contenute nelle clausole o nel contratto;

h) che, in caso di subcontratto, ha provveduto a informare l'esportatore e ha da questi ottenuto

il consenso scritto; i) che il terzo incaricato svolgerà l'attività di trattamento in conformità della

clausola 11;

j) che invierà prontamente all'esportatore copia dei subcontratti conclusi ai sensi delle presenti clausole.

Clausola 6

Responsabilità

1. Le parti convengono che l'interessato che abbia subito un pregiudizio per violazione degli obblighi di cui alla clausola 3 o alla clausola 11 ad opera di una parte o del terzo incaricato ha diritto di ottenere dall'esportatore il risarcimento del danno sofferto.

2. Qualora l'interessato non sia in grado di proporre l'azione di risarcimento di cui al paragrafo 1 nei confronti dell'esportatore per violazione di uno degli obblighi di cui alla clausola 3 o alla clausola 11 ad opera dell'importatore o del terzo incaricato, in quanto l'esportatore sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, l'importatore riconosce all'interessato stesso il diritto di agire nei suoi confronti così come se egli fosse l'esportatore, a meno che tutti gli obblighi dell'esportatore siano stati trasferiti, per contratto o per legge, all'eventuale successore, nel qual caso l'interessato può far valere i suoi diritti nei confronti del successore.

L'importatore non può far valere la violazione degli obblighi ad opera del terzo incaricato al fine di escludere la propria responsabilità.

3. Qualora l'interessato non sia in grado di agire in giudizio, ai fini dei paragrafi 1 e 2, nei confronti dell'esportatore o dell'importatore per violazione di uno degli obblighi di cui alla clausola 3 o alla clausola 11 ad opera del terzo incaricato, in quanto sia l'esportatore che l'importatore siano

scomparsi di fatto, abbiano giuridicamente cessato di esistere o siano divenuti insolventi, il terzo incaricato riconosce all'interessato stesso il diritto di agire nei suoi confronti per quanto riguarda i trattamenti da quello effettuati ai sensi delle presenti clausole così come se egli fosse l'esportatore o l'importatore, a meno che tutti gli obblighi dell'esportatore o dell'importatore siano stati trasferiti, per contratto o per legge, all'eventuale successore, nel qual caso l'interessato può far valere i suoi diritti nei confronti del successore. La responsabilità del terzo incaricato è limitata ai trattamenti da quello effettuati ai sensi delle presenti clausole.

Clausola 7

Mediazione e giurisdizione

1. L'importatore dichiara che qualora l'interessato faccia valere il diritto del terzo beneficiario e/o chieda il risarcimento dei danni in base alle presenti clausole, egli accetterà la decisione dello stesso interessato:

a) di sottoporre la controversia alla mediazione di un terzo indipendente o eventualmente

dell'autorità di controllo; b) di deferire la controversia agli organi giurisdizionali dello Stato

membro in cui è stabilito l'esportatore.

2. Le parti dichiarano che la scelta compiuta dall'interessato non pregiudica i diritti sostanziali o procedurali spettanti allo stesso relativamente ai rimedi giuridici previsti dalla normativa nazionale o internazionale.

Clausola 8

Collaborazione con le autorità di controllo

1. L'esportatore si impegna a depositare una copia del presente contratto presso l'autorità di controllo, qualora questa ne faccia richiesta o qualora il deposito sia prescritto dalla normativa sulla protezione dei dati.

2. Le parti dichiarano che l'autorità di controllo ha il diritto di sottoporre a controlli l'importatore e i subincaricati nella stessa misura e secondo le stesse modalità previste per l'esportatore dalla normativa sulla protezione dei dati.

3. L'importatore informa prontamente l'esportatore dell'esistenza di disposizioni normative applicabili all'importatore o ai subincaricati, che impediscono di sottoporli a controlli ai sensi del paragrafo 2. In tale ipotesi l'esportatore ha facoltà di prendere le misure di cui alla clausola 5, lettera b).

Clausola 9

Legge applicabile

Le presenti clausole sono soggette alla legge dello Stato membro in cui è stabilito l'esportatore, ossia .....

Clausola 10

Modifica del contratto

Le parti si impegnano a non alterare o non modificare le presenti clausole. Ciò non osta a che le parti inseriscano altre clausole commerciale ritenute necessarie, purché non siano in contrasto con le clausole.

Clausola 11

Subcontratto

1. L'importatore non può subcontrattare i trattamenti effettuati per conto dell'esportatore ai sensi delle presenti clausole senza il previo consenso scritto dell'esportatore stesso. L'importatore che, con il consenso dell'esportatore, affidi in subcontratto l'esecuzione degli obblighi ai sensi delle presenti clausole stipula, a tal fine, con il terzo incaricato un accordo scritto che imponga a quest'ultimo gli obblighi cui è egli stesso tenuto in virtù delle clausole ([1]). L'importatore rimane pienamente responsabile nei confronti dell'esportatore per l'inadempimento, da parte del terzo incaricato, degli obblighi di protezione dei dati previsti dall'accordo scritto.

2. Nell'accordo scritto tra l'importatore e il terzo incaricato è inserita la clausola del terzo beneficiario, di cui alla clausola 3, a favore dell'interessato che non sia in grado di proporre l'azione di risarcimento di cui alla clausola 6, paragrafo 1, nei confronti dell'esportatore o dell'importatore in quanto l'esportatore e l'importatore siano entrambi scomparsi di fatto, abbiano giuridicamente cessato di esistere o siano divenuti insolventi, e nessun successore abbia assunto, per contratto o per legge, l'insieme dei loro obblighi. La responsabilità civile del terzo incaricato è limitata ai trattamenti da quello effettuati ai sensi delle presenti clausole.

3. Le disposizioni sulla protezione dei dati ai fini del subcontratto di cui al paragrafo 1 sono soggette alla legge dello Stato membro in cui è stabilito l'esportatore, ossia
.....

([1]) Tale prescrizione può considerarsi soddisfatta qualora il terzo incaricato sottoscriva il contratto concluso tra l'esportatore e l'importatore ai sensi della presente decisione.

4. L'esportatore tiene un elenco dei subcontratti conclusi ai sensi delle presenti clausole e comunicati dall'importatore a norma della clausola 5, lettera j), e lo aggiorna almeno una volta all'anno. L'elenco sarà tenuto a disposizione dell'autorità di controllo dell'esportatore.

Clausola 12

Obblighi al termine dell'attività di Protezione dei dati personali

1. Le parti convengono che al termine dell'attività di trattamento l'importatore e il terzo incaricato provvedono, a scelta dell'esportatore, a restituire a quest'ultimo tutti i dati personali trasferiti e le relative copie ovvero a distruggere tali dati, certificando all'esportatore l'avvenuta distruzione, salvo che gli obblighi di legge impediscano di restituire o distruggere in tutto o in parte i dati personali trasferiti. In questo caso, l'importatore si impegna a garantire la riservatezza dei dati personali trasferiti e ad astenersi dal trattare di propria iniziativa tali dati.

2. L'importatore e il terzo incaricato si impegnano a sottoporre a controllo i propri impianti di trattamento su richiesta dell'esportatore e/o dell'autorità di controllo, ai fini della verifica dell'esecuzione dei provvedimenti di cui al paragrafo 1.

Per conto dell'esportatore:

Cognome e nome:

.....

Qualifica:

.....

Indirizzo:

.....

Altre informazioni necessarie per convalidare il contratto:


Firma ..... (timbro dell'organizzazione)

Per conto dell'importatore:

Cognome e nome:

.....

Qualifica:

.....

Indirizzo:

.....

Altre informazioni necessarie per convalidare il contratto:


Firma ..... (timbro dell'organizzazione)

Appendice 1

Alle clausole contrattuali tipo

La presente appendice costituisce parte integrante delle clausole contrattuali e deve essere compilata e sottoscritta dalle parti

(Gli Stati membri hanno facoltà di integrare o specificare ulteriormente, conformemente alle rispettive procedure nazio nali, qualsiasi altra informazione che debba fare parte della presente appendice)

Esportatore
Cliente

Importatore
Glarish,Inc.

Dati Soggetti
• Cliente

• Agente del Cliente, Dipendenti, Utenti Autorizzati

Categorie di Dati

- Identificazione dei dati:
  - nome, indirizzo, email, numero telefonico e credenziali di accesso.
- Contenuti del Cliente:
  - Immagini
  - Video
  - Documenti Power point
  - Documenti Pdf etc

Speciali catregorie di dati (se pertinenti)

Non applicabili

Tipo di Protezione dei dati

Raccolta, archiviazione, trasferimento, se necessario per la fornitura dei Servizi in base al Contratto

ESPORTATORE

NOME, COGNOME, o Nome Azienda:…….…….…….…….…….…….……(CLIENTE)

Firma Autorizzata…….…….…….…….…… …….…….……

IMPORTATORE

Nome, Cognome, Nome Azienda: Glarish,Inc.

Firma Autorizzata…….…….…….……

Appendice 2

alle clausole contrattuali tipo

La presente appendice costituisce parte integrante delle clausole contrattuali e deve essere compilata e sottoscritta dalle parti

Descrizione delle misure tecniche e organizzative di sicurezza attuate dall'importatore in conformità della clausola 4, lettera d), e della clausola 5, lettera c) (o del documento/atto legislativo allegato):

.....

.....

.....

.....

CLAUSOLA ESEMPLIFICATIVA DI INDENNIZZO (FACOLTATIVA)

Responsabilità

Le parti convengono che se una di esse viene riconosciuta responsabile di una violazione delle clausole commessa dall'altra parte, quest'ultima, nei limiti della sua responsabilità, è tenuta a indennizzare la prima per ogni costo, onere, danno, spesa o perdita sostenuti.

Tale indennizzo è subordinato al fatto che:

a) l'esportatore informi prontamente l'importatore in merito alle istanze presentate;

b) l'importatore abbia la possibilità di collaborare con l'esportatore nella difesa e nella risoluzione della controversia ([1]). ([1]) Il paragrafo sulla responsabilità è facoltativo.