ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI

"**CLIENTE**" o "**TITOLARE DEL TRATTAMENTO**":	"**MAPP**" o "**RESPONSABILE DEL TRATTAMENTO**":
Nome della ditta: _____	
Indirizzo: _____	
_____	L'entità Mapp elencata nell'Appendice 3 che è parte contraente dell'MSA.
_____	
Informazioni sull'azienda: _____	

Questo Accordo sul trattamento dei dati ("**DPA"**) fa parte del Contratto Quadro per la prestazione di servizi MAPP o di qualsiasi altro accordo per l'acquisto dei servizi di Mapp (in seguito denominato "**MSA**") tra il Cliente e Mapp.
Firmando questo DPA, il Cliente conclude il presente DPA per sé e, nella misura richiesta dalle leggi sulla protezione dei dati, in nome e per conto delle sue Affiliate.
Come sottoscrivere questo DPA:

- Se questo DPA è pre-firmato per conto di Mapp, si prega di: (1) completare le informazioni del Cliente sopra ripostate; (2) scegliere l'entità Mapp che è parte contraente del MSA; (3) rivedere l'Appendice 1 e modificarla se necessario; (3) firmare il DPA; (4) e inviare via e-mail all'indirizzo privacy@mapp.com.
- Al ricevimento del DPA debitamente sottoscritto, esso diventerà legalmente vincolante e farà parte dell'MSA.
- Se il Cliente apporta delle revisioni al presente DPA che non sono state reciprocamente concordate, tali revisioni saranno nulle. Il firmatario del Cliente dichiara a Mapp di disporre di ogni necessario potere e dell'autorità giuridica per vincolare il Cliente. Il presente DPA terminerà automaticamente nel caso di risoluzione o scioglimento per qualsiasi motivo intervenuto dell'MSA.

1. DEFINIZIONI

1.1 **Affiliata** significa qualsiasi entità che direttamente o indirettamente possiede o controlla, è posseduta o controllata da, o sotto il comune controllo o proprietà della Parte in questione.

1.2 **Legge(i) in Materia di Protezione dei Dati** si intendono tutte le leggi e regolamenti che possano esistere in qualsiasi giurisdizione pertinente, incluso: il regolamento dell'Unione europea sulla protezione e libera circolazione dei Dati Personali delle persone fisiche (il Regolamento UE 2016/679 - "Regolamento Generale sulla Protezione dei Dati" o "**RGPD**"), la Direttiva 2002/58/EC, the California Consumer Privacy Act (the "**CCPA**"), e tutte le altre leggi o regolamenti applicabili relativi o integrativi in materia di protezione dei dati, ciascuno come di volta in volta aggiornato, modificato o sostituito.

1.3 **Interessati** ha il significato attribuito dalla Legge in Materia di Protezione dei Dati;

1.4 **Violazione dei Dati Personali** indica una violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, memorizzati o comunque trattati;

1.5 **Servizi** si riferiscono agli specifici Servizi Mapp che il Cliente ha acquistato da Mapp secondo quanto stabilito dal MSA e più compiutamente descritti nell'Appendice 4.

1.6 Tutti gli altri termini indicati con la lettera maiuscola avranno il significato loro attribuito dalla Legge in Materia di Protezione dei Dati applicabile o dal MSA.

2. TRATTAMENTO DEI DATI

2.1 Le Parti riconoscono e accettano che per quanto riguarda il Trattamento dei Dati Personali, il Cliente è il Titolare del Trattamento e Mapp è il Responsabile del Trattamento.

2.2 Le Parti rispettano i rispettivi obblighi ai sensi delle Leggi in Materia di Protezione dei Dati. Ciascuna delle Parti, nel suo utilizzo dei Servizi Mapp, tratterà i Dati Personali solo in conformità con i requisiti previsti dalla Legge in Materia di Protezione dei Dati applicabile.

2.3 Le istruzioni del Cliente per il Trattamento dei Dati Personali devono essere conformi alle Leggi in Materia di Protezione dei Dati. Mapp comunicherà immediatamente al Cliente se, a suo parere, un'istruzione da parte del Cliente viola Leggi in Materia di Protezione dei Dati.

2.4 Mapp, nel suo ruolo di fornitore di servizi, tratterà i Dati Personali solo per conto e in conformità con le istruzioni documentate del Cliente ai fini di (i) Trattamento dei Dati Personali in conformità al MSA; (ii) Trattamento dei Dati Personali avviato dagli Utenti in occasione del loro utilizzo dei Servizi; (iii) Trattamento dei Dati Personali per conformarsi ad altre istruzioni documentate ragionevolmente fornite dal Cliente; (iv) tutela della riservatezza, integrità e disponibilità dei Dati Personali e dei Servizi in conformità con il presente DPA; e (v) raccolta di dati statistici che tuttavia non consentono l'identificazione degli Interessati.

2.5 Mapp agisce come fornitore di servizi al Cliente e non tratterrà, utilizzerà o divulgherà in alcun modo i Dati

Personali ad eccezione di quanto descritto nella Sezione 2.4 di cui sopra. Mapp inoltre riconosce che non venderà i Dati Personali raccolti per il tramite dei Servizi.

2.6 L'oggetto, la durata e le finalità del Trattamento e il tipo di Dati Personali e le categorie degli Interessati sono definiti nell'MSA.

3. RICHIESTE DI ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

3.1 Mapp, nella misura consentita dalla legge, informa tempestivamente il Cliente qualora dovesse ricevere una richiesta dall'Interessato per esercitare uno o più dei diritti riconosciuti dalle Leggi in Materia di Protezione dei Dati ("**Richiesta dell'Interessato"**).

3.2 Tenendo conto della natura del Trattamento dei Dati Personali, Mapp assisterà il Cliente con adeguate misure tecniche e organizzative, nella misura in cui ciò sia possibile, per l'adempimento dell'obbligo del Cliente di rispondere a una Richiesta dell'Interessato ai sensi delle Leggi in Materia di Protezione dei Dati.

3.3 Qualora il Cliente, nel suo utilizzo dei Servizi, non abbia la capacità di rispondere a una Richiesta dell'Interessato, Mapp farà, su richiesta del Cliente, ogni sforzo commercialmente ragionevole per aiutare il Cliente a rispondere a tale Richiesta dell'Interessato, nella misura in cui Mapp sia legalmente autorizzato a farlo e la risposta a tale Richiesta dell'Interessato sia prevista dalle Legge in Materia di Protezione dei Dati. Nella misura consentita dalla legge, il Cliente sarà responsabile di eventuali costi derivanti dalla fornitura di tale assistenza da parte di Mapp.

4. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Mapp fornirà al Cliente l'assistenza ragionevole con le eventuali valutazioni d'impatto sulla protezione dei dati e consultazioni preventive con l'Autorità di Controllo, richieste ai sensi delle Leggi in Materia di Protezione dei Dati, in ogni caso esclusivamente in relazione al Trattamento dei Dati Personali, e tenendo conto della natura del Trattamento e delle informazioni a disposizione di Mapp.

5. COMUNICAZIONE DELLA VIOLAZIONE DEI DATI PERSONALI

5.1 Mapp darà tempestiva comunicazione al Cliente di qualsivoglia Violazione dei Dati Personali dopo esserne venuto a conoscenza. Mapp fornirà al Cliente le informazioni sufficienti per consentire al Cliente di adempiere a qualsiasi obbligo di notifica della Violazione dei Dati Personali all'Autorità di Controllo e/o di comunicazione della Violazione dei Dati Personali agli Interessati ai sensi della Legge in Materia di Protezione dei Dati applicabile.

5.2 Mapp dovrà compiere ogni ragionevole sforzo per identificare la causa della Violazione dei Dati Personali e prendere quei provvedimenti che ritiene necessari e ragionevoli al fine di rimediare alla causa di tale Violazione di Dati Personali del Cliente nella misura in cui l'adozione di tali provvedimenti rientri nel ragionevole controllo di Mapp.

5.3 Gli obblighi di cui al presente DPA non si applicano agli incidenti causati dal Cliente.

6. SUB-TRATTAMENTO

6.1 Le Affiliate di Mapp e gli altri sub-responsabili utilizzati da Mapp per fornire i propri Servizi contrattuali, compreso il loro ruolo e ambito nonché l'area geografica di riferimento, sono individuati nell'elenco dei sub-responsabili di Mapp disponibile all'Appendice 3 e/o accessibile all'indirizzo www.mapp.com/contracts. La presente vale quale autorizzazione generale per Mapp a nominare sub-responsabili. Mapp informerà il Cliente di eventuali modifiche al predetto elenco, riguardanti l'aggiunta o la sostituzione di altri sub-responsabili del Trattamento, dando così al Cliente l'opportunità di opporsi a tali modifiche così come previsto alla successiva Sezione 6.4. Con la sottoscrizione del presente DPA, il Cliente accetta l'elenco dei sub-responsabili qui allegato come Appendice 3 e con la presente autorizza Mapp a trasferire i Dati Personali alle Affiliate di Mapp elencate e/o ad altri sub-responsabili collocati al di fuori dello Spazio Economico Europeo (SEE), come ragionevolmente richiesto al fine di fornire supporto, realizzare progetti tecnici o fornire altre tipologie di servizi nell'ambito del MSA, a condizione che, se il Cliente ha sede nell'UE: (i) tali paesi al di fuori dello SEE siano riconosciuti dalla Commissione Europea in quanto forniscono garanzie adeguate di protezione dei Dati Personali; o (ii) Mapp abbia sottoscritto le clausole contrattuali standard dell'UE con tali Affiliate e/o altri sub-responsabili.

6.2 Mapp ha stipulato un accordo scritto con ciascun sub-responsabile contenente obblighi di protezione dei Dati Personali non meno protettivi rispetto a quelli di cui al presente DPA in relazione alla protezione dei Dati Personali nella misura applicabile alla natura dei Servizi forniti da tale sub-responsabile.

6.3 Mapp sarà responsabile degli atti e delle omissioni dei suoi sub-responsabili nella stessa misura in cui Mapp sarebbe responsabile se eseguisse i servizi di ciascun sub-responsabile direttamente ai sensi del presente DPA, salvo quanto diversamente stabilito nel MSA.

6.4 Nel caso che Mapp necessiti di modificare o aggiungere un sub-responsabile al predetto elenco, Mapp informerà il Cliente. Il Cliente avrà il diritto di opporsi a qualsiasi eventuale aggiunta o sostituzione del/dei sub-responsabile/i entro un ragionevole lasso di tempo. Laddove il Cliente non dovesse opporsi a tale aggiunta o sostituzione entro tale periodo di tempo, si riterrà che il Cliente abbia acconsentito a tale cambiamento. Laddove esista una ragione di concreta rilevanza per tale opposizione, e in mancanza di una risoluzione amichevole della questione, il Cliente avrà il diritto di terminare il DPA. Mapp garantirà che ogni nuovo sub-responsabile sia tenuto

al rispetto dei medesimi obblighi di protezione dei Dati Personali applicabili ai sub-responsabili precedentemente nominati.

7. SICUREZZA

Tenuto conto delle conoscenze tecniche, dei costi di implementazione e della natura, della portata, del contesto e delle finalità del Trattamento nonché del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, Mapp deve mantenere gli adeguati requisiti tecnici e organizzativi per la protezione della sicurezza (compresa la protezione contro il Trattamento non autorizzato o illecito e contro la distruzione, la perdita o l'alterazione accidentale o illecita, la divulgazione non autorizzata o l'accesso ai Dati Personali del Cliente), la riservatezza e l'integrità dei Dati Personali, come stabilito nell'allegato sulla sicurezza di Mapp (Appendice 2 del presente DPA). Mapp controlla regolarmente la conformità con queste misure. Mapp non ridurrà in maniera sostanziale la sicurezza complessiva dei Servizi durante la durata del MSA. Mapp limiterà l'accesso ai Dati Personali ai propri dipendenti o sub-responsabili per i quali l'accesso a tali dati è ragionevolmente necessario per adempiere agli obblighi di Mapp verso il Cliente. Mapp dovrà garantire che le persone autorizzate a trattare i Dati Personali siano vincolate dagli stessi obblighi di riservatezza di Mapp o a obblighi di riservatezza equivalenti, o che siano soggetti ad un obbligo legale di riservatezza appropriato. La Policy di Sicurezza delle Informazioni è messa da Mapp a disposizione del Cliente previa sua richiesta, qualora il Cliente avesse necessità di ricevere ulteriori dettagli relativi a questa sezione.

8. CANCELLAZIONE O RETTIFICA DEI DATI PERSONALI

8.1 Mapp cancellerà i Dati Personali al termine/scadenza del MSA come specificato nel MSA o su richiesta ragionevole del Cliente entro 30 giorni, e assicurerà che i dati cancellati non siano recuperabili. Mapp potrà conservare i Dati Personali esclusivamente nella misura e per il periodo richiesto dalle leggi applicabili e sempre a condizione che Mapp garantisca la riservatezza di tali Dati Personali e che tali Dati Personali siano solo trattati, se necessario, esclusivamente per gli scopi specificati nelle leggi applicabili che ne richiedono la conservazione.

8.2 Mapp fornirà al Cliente, dietro sua richiesta, conferma scritta che la cancellazione è avvenuta in conformità con la presente sezione 8.

8.3 Mapp restituirà i Dati Personali al Cliente secondo la procedura e i tempi specificati nel MSA.

9. AUDIT E ISPEZIONI

9.1 Mapp mette a disposizione del Cliente tutte le informazioni necessarie a dimostrare il rispetto del presente DPA, nonché consente e contribuisce allo svolgimento di attività di audit da parte del Cliente o di un un revisore terzo incaricato dal Cliente, in relazione al Trattamento dei Dati Personali. Su richiesta scritta del Cliente, Mapp dovrà, non più di una volta all'anno, completare accuratamente un questionario sulla sicurezza delle informazioni fornito dal Cliente, relativo alle pratiche e alle politiche di protezione dei dati e della sicurezza delle informazioni adottate da Mapp.

9.2 Il Cliente o un revisore terzo incaricato dal Cliente può, a spese del Cliente e non più di una volta l'anno, eseguire attività di audit in loco circa le pratiche e le politiche di protezione dei dati e della sicurezza delle informazioni di Mapp, previo invio di una comunicazione scritta da trasmettersi con un preavviso ragionevole, non inferiore a dieci giorni lavorativi. L'ispezione deve svolgersi in un solo giorno durante il normale orario di lavoro di Mapp, sulla base di un programma previamente concordato che riduca al minimo l'impatto dell'audit sulle operazioni di Mapp. Il Cliente o il revisore esterno incaricato dal Cliente deve attenersi ai requisiti di sicurezza di Mapp relativi all'esecuzione dell'ispezione. A causa dei requisiti di riservatezza e sicurezza, tali ispezioni devono escludere ispezioni in loco di ambienti multi-tenant (come i centri di dati IaaS utilizzati da Mapp). Le ispezioni in loco di tali ambienti possono essere sostituite da una documentazione dettagliata riguardante le rispettive misure di protezione dei Dati Personali e di sicurezza adottate e certificazioni specifiche rilasciate da affidabili revisori esterni, fornite da Mapp su richiesta del Cliente.

9.3 Il Cliente deve prontamente informare Mapp di qualsiasi inadempienza riscontrata durante tale verifica/ispezione.

10. RESPONSABILITÀ

10.1 La responsabilità di ciascuna delle Parti derivante da o correlata al presente DPA e tutti i DPA in essere tra le Affiliate e Mapp, sia essa una responsabilità di natura contrattuale, extracontrattuale o di qualsivoglia altra natura, è soggetta alla relativa sezione del MSA concernente la limitazione di responsabilità e qualsiasi riferimento in tale sezione alla responsabilità di una Parte significa la responsabilità aggregata di quella Parte e di tutte le sue Affiliate ai sensi dell'MSA e complessivamente di tutti i DPA.

10.2 A scanso di equivoci, la responsabilità totale di Mapp per tutte le richieste di risarcimento da parte del Cliente e di tutte le sue Affiliate derivanti da o correlate al MSA e ad ogni DPA si applica in forma aggregata per tutte le rivendicazioni ai sensi sia del MSA sia di tutti i DPA stabiliti ai sensi di questo accordo.

10.3 Laddove un Interessato faccia valere qualsivoglia diritto nei confronti di una Parte di questo DPA ai sensi della Legge in Materia di Protezione dei Dati applicabile, l'altra Parte fornirà, ove possibile, il proprio supporto nella difesa contro tali richieste.

Appendice 1: **Interessati e categorie di Dati Personali**
Appendice 2: **Allegato sulla sicurezza**
Appendice 3: **Elenco delle Affiliate e dei Sub-responsabili di Mapp**
Appendice 4: **Descrizione dei Servizi di Mapp**

TITOLARE DEL TRATTAMENTO		**RESPONSABILE DEL TRATTAMENTO**	
Firma:		Firma:	
Nome stampato, qualifica:		Nome stampato, qualifica:	Steven Warren, CEO
Data:		Data:	

APPENDICE 1: INTERESSATI E CATEGORIE DI DATI PERSONALI

Gli Interessati cui si riferiscono i Dati Personali. I Dati Personali trattati riguardano le seguenti categorie di Interessati:

- clienti del Cliente,
- clienti potenziali del Cliente,
- Visitatori del sito web del Cliente,
- Dipendenti del Cliente.

Categorie cui si riferiscono i Dati Personali. I Dati Personali trattati riguardano le seguenti categorie:

- Indirizzi email,
- Numero di cellulare,
- Numero di rete fissa,
- Cognome, nome,
- Indirizzo postale,
- Data di nascita,
- Apertura delle e-mail ricevute,
- Clic di collegamenti all'interno delle e-mail ricevute,
- Indirizzi IP,
- Comportamento di utilizzo del sito web.

APPENDICE 2: ALLEGATO SULLA SICUREZZA

MISURE DI SICUREZZA DELLE INFORMAZIONI TECNICHE E ORGANIZZATIVE VERSIONE 5.0, 23-05-2019

1. Riservatezza (Art. 32 Sez. 1 lettera a e b GDPR e art. 25 cpv. 1 GDPR))	
Controllo di accesso fisico	**Implementazione**
Mapp manterrà misure adeguate al fine di impedire a persone non autorizzate di accedere alle apparecchiature di trattamento dei dati qualora i dati personali siano trattati o utilizzati.	Le misure sono progettate, applicate e monitorate in conformità con gli standard ISO 27001:2013, in particolare dall'A.11.1.x fino all'A.11.6.x. Queste includono: - Stabilite aree di sicurezza con punti di ingresso/uscita protetti. - Procedure di autorizzazione per dipendenti e terze parti. - Procedure di gestione dei visitatori per garantire un'idonea autenticazione e supervisione. - Monitoraggio TVCC per tutti i centri di dati e le sedi degli uffici primari che coprono tutti i punti di ingresso e di uscita. - L'accesso alle apparecchiature del centro di dati richiede come minimo due diversi fattori di autenticazione. - Le apparecchiature sono installate per proteggerle in modo efficace dalla divulgazione non autorizzata delle informazioni. - Sistemi di allarme di sicurezza per i centri di dati e le sedi di uffici primari. - Ricezione in presenza di operatori e/o agenti di sicurezza nei centri di dati. - Procedure per l'assegnazione sicura delle chiavi di accesso e/o l'iscrizione dei dati biometrici. - Sistema di accesso elettronico che registra tutti gli accessi ai centri di dati e alle sedi degli uffici primari. - Ulteriori controlli di sicurezza secondo le politiche di sicurezza delle informazioni di Mapp.
Controllo dell'accesso al sistema	**Implementazione**
Mapp manterrà misure adeguate per impedire che i suoi sistemi di trattamento dei dati personali vengano utilizzati da persone non autorizzate.	Le misure sono progettate, applicate e monitorate in conformità con gli standard ISO 27001:2013, in particolare A.6.2.1, A.9.1.x, A.9.2.x, A.9.3.x, A.10.1.x, A.11.2.8-.9, A.12.2.1, A.12.4.1, A.12.6.1, A.14.2.x e A.18.2.3. Queste includono: - Mantenimento della politica di controllo accessi. - Procedura per la gestione di account utente e privilegiati in linea con il ciclo di vita occupazionale basato su una directory centrale. - Autenticazione a più fattori richiesta per l'accesso privilegiato all'infrastruttura. - Politica per le password che richiede tecnicamente almeno 8 caratteri; includere almeno tre dei seguenti quattro elementi: lettere maiuscole, lettere minuscole, numeri, simboli; una password diversa dalle 8 precedentemente utilizzate; le password utente interne scadono dopo 90 giorni; e una lunghezza minima per account di amministratore e di servizio di 14 caratteri. Gli utenti sono tenuti a cambiare le password iniziali al primo accesso. - I dipendenti sono tenuti a seguire la politica della "scrivania pulita" (c.d. *clean desk policy*). Le schermate vengono bloccate automaticamente dopo non più di 15 minuti di inattività. - L'accesso alla rete interna è limitato ai dispositivi aziendali autorizzati. - I sistemi anti-malware installati su tutti i sistemi Windows e server Linux che sono suscettibili alle infezioni da malware. - Monitoraggio di eventi di sicurezza relativi a sistemi interni e di produzione. - Nessun trattamento dei dati su dispositivi mobili come telefoni cellulari o tablet. - Politica che vieta il trasferimento di dati su supporti rimovibili. - Il Cliente rimane responsabile della protezione delle credenziali sotto il suo controllo. - Processo per la gestione della vulnerabilità tecnica, compresa l'analisi del codice statico, valutazioni periodiche della vulnerabilità interna e test di penetrazione di terze parti. I Clienti possono condurre le proprie valutazioni tecniche in accordo con Mapp. - Principi di codifica sicuri secondo OWASP Top 10, che vengono regolarmente forniti agli sviluppatori di software. - Le reti di produzione sono efficacemente segregate e protette da firewall. Nessuna archiviazione di dati nell'area di presentazione di una rete. - Sistema di rilevamento delle intrusioni basato su host installato e monitorato (applicabile a Mapp Engage). - Sistema di rilevamento e prevenzione delle intrusioni basato sulla rete installato e monitorato (applicabile a Mapp Engage). - Ulteriori controlli di sicurezza secondo le politiche di sicurezza delle informazioni di Mapp.
Controllo dell'accesso ai dati	**Implementazione**
Nessuna operazione di lettura, copia, modifica o cancellazione non autorizzata all'interno dei sistemi informativi	Le misure sono progettate, applicate e monitorate conformemente agli standard ISO 27001:2013, in particolare A.6.2.1, A.8.3.2, A.9.1.x, A.9.2.x, A.10.1.1-.2, e A.11.2.7. Queste includono: - Procedura per la gestione dei diritti di accesso utente e privilegiati in linea con il ciclo di vita occupazionale basato su una directory centrale. - Accesso ai dati riservati ai gruppi autorizzati. - L'assegnazione dei diritti di accesso privilegiato segue il principio del minimo privilegio. - Ruolo granulare e modello di autorizzazione implementati per consentire la personalizzazione dell'accesso dei Clienti in base al principio della necessità di sapere. - Gli account degli elenchi centrali vengono rivisti con cadenza semestrale. - Gli account privilegiati con accesso all'infrastruttura vengono rivisti almeno una volta l'anno. - L'attività dell'utente e dell'account privilegiato, così come altri eventi relativi alla sicurezza, vengono registrati e i registri protetti da perdita e manipolazione. - I registri degli account privilegiati vengono regolarmente esaminati, manualmente e/o automaticamente. - Il Cliente rimane responsabile delle revisioni di accesso specifiche dell'applicazione, dell'accuratezza della lista di controllo degli accessi e della protezione delle credenziali assegnate.

	- I sistemi di archiviazione applicano la crittografia a livello di filesystem od oggetto usando AES-256 (o equivalente, applicabile a Mapp Engage e a Mapp Acquire). - Utilizzo di filesystem crittografati su laptop aziendali. - Utilizzo di supporti rimovibili tecnicamente limitati. - Procedure per lo smaltimento sicuro delle apparecchiature e cancellazione irreversibile dei dati nel corso della rimozione dei diritti di accesso del Cliente. - Ulteriori controlli di sicurezza secondo le politiche di sicurezza delle informazioni di Mapp.
Controllo di separazione	**Implementazione**
Elaborazione separata dei dati raccolti per scopi diversi.	Le misure sono progettate, applicate e monitorate conformemente agli standard ISO 27001:2013, in particolare A.9.4.1, A.12.1.4 e A14.3.1. Queste includono: - Segregazione logica dei dati dei locatari negli ambienti di produzione e di servizio. - Lo sviluppo e i sistemi di prova sono separati dagli ambienti di produzione. - Nessun utilizzo dei dati di produzione a scopo di test. - Ulteriori controlli di sicurezza secondo le politiche di sicurezza delle informazioni di Mapp.
Pseudonimizzazione	**Implementazione**
Trattamento dei dati personali in un modo che impedisce l'associazione dei dati a un determinato individuo senza ulteriori informazioni che vengono mantenute separatamente da adeguate misure tecniche o organizzative.	Le misure sono progettate, applicate e monitorate conformemente agli standard ISO 27001:2013, in particolare A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.8. Queste includono: - Le procedure di sviluppo comprendono i principi di progettazione per la minimizzazione dei dati, la limitazione della raccolta e la privacy per impostazione predefinita, incluso il requisito per la pseudonimizzazione laddove possibile. - I dati comportamentali sono archiviati in forma pseudonomizzata e separati dal profilo di contatto corrispondente laddove possibile (si applica a Mapp Engage). - Tracking online per pseudonimo predefinito, opzione per pseudonimizzare e anonimizzare gli attributi personalizzati raccolti, ad es. tramite indirizzamento calcolato o troncamento (si applica a Mapp Acquire e a Mapp Intelligence). - I log di sistema sono resi anonimi laddove possibile. - Ulteriori controlli di sicurezza secondo le politiche di sicurezza delle informazioni di Mapp.
2. Integrità (Art. 32 Sez. 1 lettera b GDPR)	
Controllo del trasferimento	**Implementazione**
Nessuna operazione di lettura, copia, modifica o cancellazione non autorizzata durante la trasmissione o il trasporto.	Le misure sono progettate, applicate e monitorate conformemente agli standard ISO 27001:2013, in particolare A.8.3.3, A.9.1.x e A.10.1.1-2. Queste includono: - I dati trasferiti sulle reti pubbliche di trasmissione dei dati sono protetti efficacemente utilizzando standard e algoritmi di buone pratiche del settore come TLS o SSH con configurazioni sicure. - I dati non vengono trasferiti fisicamente, né su carta né su dispositivi di archiviazione mobile. - Sono disponibili funzionalità di messaggistica elettronica sicure per le comunicazioni interne ed esterne, ma non consentiamo il trasferimento di dati (trattati in base a questo DPA) via email. Nel caso in cui i Clienti inviino dati via e-mail o incarichino Mapp per farlo, il Cliente sarà ritenuto responsabile. - Ulteriori controlli di sicurezza secondo le politiche di sicurezza delle informazioni di Mapp.
Controllo di ingresso	**Implementazione**
Determinazione se i dati personali sono stati inseriti, modificati o cancellati dai sistemi informativi.	Le misure sono progettate, applicate e monitorate in base agli standard ISO 27001:2013, in particolare A.12.2.1, A.12.4.1-.4 e A.12.6.1. Queste includono: - Gli account utente e privilegiati sono unici e identificabili laddove tecnicamente fattibile; eccezione: account root che sono strettamente controllati. - L'accesso ai dati a livello di applicazione e di database viene registrato in modo completo e i registri sono protetti dalla perdita e dalla manipolazione. - Le fonti log utilizzano un'origine ora sincronizzata (NTP). - Sistema di rilevamento delle intrusioni basato su host installato e monitorato (applicabile a Mapp Engage). - Sistema di rilevamento e prevenzione delle intrusioni basato sulla rete installato e monitorato (applicabile a Mapp Engage). - Processo per la gestione della vulnerabilità tecnica, compresa l'analisi del codice statico, valutazioni periodiche della vulnerabilità interna e test di penetrazione di terze parti. I Clienti possono condurre le proprie valutazioni tecniche in accordo con Mapp. - I sistemi anti-malware installati su tutti i sistemi Windows e server Linux che sono suscettibili alle infezioni da malware. - Ulteriori controlli di sicurezza secondo le politiche di sicurezza delle informazioni di Mapp.
3. Disponibilità e resilienza (Art. 32 Sez. 1 lettera b e c GDPR)	
Controllo della disponibilità	**Implementazione**
Protezione contro perdite o distruzioni accidentali o intenzionali.	Le misure sono progettate, applicate e monitorate conformemente agli standard ISO 27001:2013, in particolare A.12.1.2, A.12.1.3, A.12.2.1, A.12.3.1, A.12.4.1, A.12.6.1, A.17.1.x, e A.17.2.1. Queste includono: - I sistemi di rilevamento e soppressione sono implementati nei centri di dati per ridurre al minimo i rischi legati al fuoco e all'acqua. Questi sono conservati e testati almeno una volta l'anno. - L'equipaggiamento è installato per proteggerlo efficacemente da danni ambientali o sabotaggio. - I componenti critici del sistema (es. server Web o equilibratori di carico) sono disposti in modo ridondante per evitare singoli punti di errore. - I dati vengono replicati e i dati relazionali vengono sottoposti a backup quotidianamente. - Processo per la gestione della vulnerabilità tecnica, compresa l'analisi del codice statico, valutazioni periodiche della vulnerabilità interna e test di penetrazione di terze parti. I Clienti possono condurre le proprie valutazioni tecniche in accordo con Mapp. - Pianificazione e monitoraggio delle capacità di elaborazione, archiviazione e rete. - Monitoraggio della salute e della disponibilità del sistema. - Procedure per la gestione delle modifiche durante le normali operazioni e le emergenze.

	- I sistemi anti-malware installati su tutti i sistemi Windows e server Linux che sono suscettibili alle infezioni da malware. - Sistema di rilevamento e prevenzione delle intrusioni basato sulla rete installato e monitorato per proteggere dagli attacchi finalizzati al diniego di servizi (si applica a Mapp Engage). - Ulteriori controlli di sicurezza secondo le politiche di sicurezza delle informazioni di Mapp.
Capacità di recupero	**Implementazione**
Capacità di recupero entro un periodo di tempo appropriato dopo un evento di disturbo.	Le misure sono progettate, applicate e monitorate conformemente agli standard ISO 27001:2013, in particolare A.12.3.1, A.17.1.x e A.17.2.1. Queste includono: - I piani di continuità operativa e di ripristino in caso di incidente per centri di dati e servizi software vengono conservati e testati regolarmente. - UPS e generatori diesel sono implementati nei centri di dati per sopravvivere alle interruzioni di corrente di almeno 24 ore. Questi sono conservati e testati almeno una volta l'anno. - I dati vengono replicati e i dati relazionali vengono sottoposti a backup quotidianamente. Le procedure di recupero del backup vengono regolarmente testate. - Ulteriori controlli di sicurezza secondo le politiche di sicurezza delle informazioni di Mapp.
4. Processo per la valutazione periodica dell'efficacia delle misure (Art. 32 Sez. 1 lettera d GDPR; Art. 25 sez. 1 e 2 GDPR)	
Gestione della protezione dei dati	**Implementazione**
Approccio sistematico alla gestione della protezione dei dati.	Funzionamento di un sistema di gestione della sicurezza delle informazioni e della protezione dei dati in conformità agli standard ISO 27001:2013, ISO 27002:2013, e ISO 27018:2014. Ciò comprende: - Ruoli e responsabilità chiaramente definiti e comunicati in materia di sicurezza delle informazioni e privacy, inclusi ma non limitati a: Responsabile della sicurezza delle informazioni e Responsabile della protezione dei dati / della privacy. - Procedure di governance per la gestione del rischio informatico, manutenzione e comunicazione delle politiche, valutazioni di conformità interne e di terzi, reportistica e revisione della gestione e tracciamento del miglioramento continuo. - Programma per la sicurezza delle informazioni e la tutela della privacy che include nuovi corsi di formazione obbligatori e annuali di aggiornamento e ulteriori misure di sensibilizzazione. - Audit annuale indipendente del sistema di gestione della sicurezza delle informazioni e della protezione dei dati. - Ulteriori controlli di sicurezza secondo le politiche di sicurezza delle informazioni di Mapp.
Gestione della risposta agli incidenti	**Implementazione**
Approccio sistematico alla gestione degli incidenti.	Le misure sono progettate, applicate e monitorate conformemente agli standard ISO 27001:2013, in particolare A.16.1.x. Queste includono: - Procedura per la segnalazione degli incidenti, fornita a tutti i dipendenti. - Procedura per la risposta agli incidenti inclusa verifica, classificazione, contenimento, eradicazione e recupero; playbook mantenuti per determinati tipi di incidenti. - Procedura per la notifica in linea con i requisiti legali e contrattuali. - Analisi post-mortem richiesta per incidenti significativi. - Ulteriori controlli di sicurezza secondo le politiche di sicurezza delle informazioni di Mapp.
Privacy per impostazione predefinita (Privacy by default)	**Implementazione**
La conformità alla protezione dei dati dovrebbe essere integrata durante l'intero ciclo di vita delle tecnologie e delle procedure.	Le misure sono progettate, applicate e monitorate conformemente agli standard ISO 27001:2013, in particolare A.8.1.3, A.13.2.1 e A.14.2.5. Queste includono: - Le procedure di sviluppo includono i principi di progettazione per la minimizzazione dei dati, la limitazione della raccolta e la privacy per impostazione predefinita (*privacy by default*). I nostri servizi software sono altamente personalizzabili. Le opzioni per la configurazione sono disponibili nella rispettiva guida online. - I Clienti rimangono responsabili per l'uso legale e rispettoso della privacy dei servizi software di Mapp. Inoltre, si applica la Acceptable Use Policy (Politica di Utilizzo Accettabile) disponibile al seguente URL: https://mapp.com/acceptable-use-policy/
Controllo degli ordini (articolo 28 GDPR)	**Implementazione**
Nessun trattamento dei dati senza le istruzioni del responsabile del trattamento.	Le misure sono progettate, applicate e monitorate conformemente agli standard ISO 27001:2013, in particolare A.8.3.2, A.11.2.7, A.13.2.1 e A.18.1.1. Queste includono: - Mapp tratta i dati dei solo in base alle istruzioni del Cliente, ovvero in base ad accordi contrattuali, ordini o istruzioni aggiuntive. I Clienti devono fornire istruzioni solo in forma scritta o confermare in forma scritta quando fatto verbalmente. - Procedure per lo smaltimento sicuro delle apparecchiature e cancellazione irreversibile dei dati nel corso della rimozione dei diritti di accesso del Cliente. - Limitazione effettiva del trattamento dei dati conservati per scopi legali tramite crittografia dei file di backup, crittografia dei file system, severi controlli di accesso, registrazione di audit e procedure di ripristino basate sui ticket.

APPENDICE 3: ELENCO DEGLI AFFILIATI E DEI SUBRESPONSABILI DI MAPP

	Sub-responsabile	Luogo in cui i Dati Personali vengono Trattati (e garanzie legali, se al di fuori del SEE)	Finalità
ENTITÀ MAPP	Mapp Digital Germany GmbH	Germania	Interno: supporto e servizi, ricerca e sviluppo
	Mapp Digital France SAS	Francia	Interno: supporto e servizi
	Mapp Digital Italy SrL.	Italia	Interno: supporto e servizi
	Mapp Digital UK Ltd	Regno Unito*(Clausole contrattuali standard dell'UE)	Interno: supporto e servizi
	Mapp Digital Poland sp. zoo	Polonia	Interno: Ricerca e sviluppo
	Mapp Digital Netherlands BV	Olanda	Interno: Ricerca e sviluppo
	Mapp Digital US, LLC	Stati Uniti (clausole contrattuali standard dell'UE e Certificazione ai sensi dello UE-USA Privacy Shield)	Interno: supporto e servizi, ricerca e sviluppo [solo Mapp Empower]
	Webtrekk GmbH	Germania e Italia	Interno: supporto e servizi, ricerca e sviluppo
AFFILIATA	Aprimo Australia Pty Ltd	Australia (Clausole contrattuali standard dell'UE)	Interno: supporto
TERZE PARTI ESTERNE	Pythian Group Inc.	Canada (Decisione di adeguatezza)	Esterno: ricerca e sviluppo [solo Mapp Empower]
	Amazon Web Services, Inc.	Germania e Irlanda	Esterno: infrastruttura del centro di dati
	Amazon Web Services, Inc.	Stati Uniti (Clausole contrattuali standard dell'UE)	Esterno: infrastruttura del centro di dati [solo Mapp Empower]
	Google, LLC.	Trattamento principale e archiviazione dei dati in Belgio. Raccolta globalmente distribuita tecnicamente necessaria a causa della natura dei Servizi (Clausole contrattuali standard dell'UE)	Esterno: Infrastruttura del centro di dati [solo Mapp Acquire]
	Accesso globale Internet Servizi GmbH	Germania	Esterno: infrastruttura del centro di dati
	CLX Networks AB	Svezia e Stati Uniti (Clausole contrattuali standard dell'UE)	Esterno: SMS [Mapp Engage, opzionale]
	R & D Communications Srl	Italia	Esterno: SMS [Mapp Engage, opzionale]
	Mitto AG	Germania e Svizzera (Decisione di adeguatezza)	Esterno: SMS [Mapp Engage, opzionale]
	QSC AG	Germania	Esterno: Infrastruttura del centro di dati [solo Mapp Intelligence]

*Nel caso in cui il Regno Unito diventi un paese terzo nel corso della Brexit, Mapp ha sottoscritto clausole contrattuali standard per garantire la conformità futura dei trasferimenti transfrontalieri di Dati Personali.

I FORNITORI SUPPLEMENTARI POSSONO ESSERE NECESSARI PER DETERMINATI SERVIZI O PER QUEI CLIENTI CON DOMANDE DI SUPPORTO ELEVATE. QUESTI FORNITORI DEVONO ESSERE DESIGNATI NELLE SPECIFICHE DEL LAVORO APPLICABILI PER QUESTI SERVIZI.

APPENDICE 4: DESCRIZIONE DEI SERVIZI DI MAPP

Mapp Cloud include i seguenti Servizi, che possono essere acquistati separatamente:

Mapp Engage

Mapp Engage è una soluzione basata sul cloud per la creazione, la pianificazione e l'erogazione di campagne pubblicitarie e altre comunicazioni di clienti e clienti potenziali attraverso e-mail, app, social e canali web. Le funzionalità complete di segmentazione del gruppo di destinazione si basano sulle interazioni e gli attributi degli utenti acquisiti nei canali supportati. Per uno stile di lavoro basato sui dati, sono disponibili anche pannelli di controllo grafici per monitorare il successo e ottimizzare ulteriormente le attività di comunicazione.

Mapp Intelligence

Mapp Intelligence è una soluzione cloud per la raccolta, l'analisi e l'attivazione di dati di prime parti. I dati vengono raccolti sui siti web della società, sulle applicazioni e su altri canali digitali utilizzando librerie di monitoraggio (SDK – Library software development) sviluppate in-house. Per valutare tali dati sono disponibili diversi strumenti di analisi, che consentono di visualizzare tendenze a lungo termine, anomalie e altri risultati. I dati e gli insight acquisiti possono essere messi a disposizione di altri prodotti all'interno di Mapp Cloud, ma anche di sistemi esterni, ai fini della comunicazione e del marketing.

Mapp Acquire

La soluzione cloud Mapp Acquire consente la raccolta di dati di prime parti su siti web e applicazioni mobile. La raccolta di dati può essere configurata nel modo desiderato e comprende gli attributi dell'utente, le interazioni con il sito web o l'app e le transazioni. I dati vengono utilizzati per personalizzare le comunicazioni dei clienti e vengono messi a disposizione degli altri prodotti di Mapp Cloud per questo scopo. Facoltativamente, i dati possono essere utilizzati in terzi canali, ad esempio per scopi di retargeting nelle reti pubblicitarie di Google e Facebook.

Mapp Empower

Mapp Empower è una soluzione di email marketing per inviare campagne email ad aziende clienti e clienti potenziali. Sono raccolti gli indirizzi email e attributi opzionali dell'utente vengono per esempio il nome e sesso dell'utente. I dati vengono utilizzati per personalizzare le comunicazioni destinate ad aziende clienti e clienti potenziali.

POSIZIONE DEI DATI DEL PRODOTTO (I dati sono comunque accessibili da altre ubicazioni secondo le disposizioni del DPA)	
PRODOTTO	**POSIZIONE DI HOSTING DATI**
Mapp Engage	Germania
Mapp Acquire	Belgio
Mapp Intelligence	Germania
Mapp Empower	Stati Uniti