ACCORDO SUL TRATTAMENTO DEI DATI

"**CLIENTE**" o "**RESPONSABILE DEL TRATTAMENTO**":	"**MAPP**" o "**INCARICATO DEL TRATTAMENTO**":
Nome della ditta: _____	
Indirizzo: _____	
_____	L'ente Maap elencato nell'appendice 3 che è parte contraente dell'MSA.
_____	
Informazioni sull'azienda: _____	

Questo Accordo sul trattamento dei dati ("**DPA"**) fa parte dell'Accordo Quadro per la prestazione di servizi MAPP o di altro accordo per l'acquisto dei servizi di Mapp (in seguito denominato " **MSA** ") tra Cliente e Mapp.
Firmando questo DPA, il Cliente entra in questo DPA per conto proprio e, nella misura richiesta dalle leggi e dai regolamenti sulla protezione dei dati, in nome e per conto delle sue affiliate.
Come eseguire questo DPA:

- Se questo DPA è pre-firmato per conto di Mapp, si prega di: (1) completare le informazioni del Cliente sopra; (2) scegliere l'ente Mapp che è parte contraente dell'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 pienamente eseguito, 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 dell'autorità giuridica per vincolare il Cliente. Il presente DPA terminerà automaticamente nel caso di risoluzione dell'MSA.

1. DEFINIZIONI

1.1 **Affiliata** significa qualsiasi entità che direttamente o indirettamente possiede o controlla, è posseduta o controllata da, o è di proprietà comune o di controllo comune con la parte in questione.

1.2 **Direttiva** indica la Direttiva UE 95/46/CE sulla protezione dei dati.

1.3 **Legislazione sulla protezione dei dati** indica le direttive europee 95/46/CE e 2002/58 CE, GDPR (regolamento (UE) 2016/679), qualsiasi legislazione e/o regolamento attuativo o emanato in conformità ad esse che modifica, sostituisce, rimette in vigore, attua, consolida o deroga da uno di esse e tutte le altre leggi applicabili relative al trattamento dei dati personali e alla privacy che possono esistere in qualsiasi giurisdizione pertinente, inclusi, se del caso, le linee guida e i codici di condotta rilasciati di volta in volta da Autorità per la protezione dei dati, altre autorità di controllo della protezione dei dati competenti a livello nazionale e del gruppo in tutto il territorio nazionale, la Commissione europea, il Gruppo di lavoro di cui all'articolo 29 e il comitato europeo per la protezione dei dati.

1.4 **Per Leggi e regolamenti sulla protezione dei dati** si intende qualsiasi legislazione e regolamento subordinati che attuino la Direttiva che può essere applicata, dal 25 maggio 2018 e in seguito, e il regolamento dell'Unione europea sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati e abrogazione della direttiva 95/46/CE (il "**Regolamento generale sulla protezione dei dati"** o "**GDPR"**) e qualsiasi legislazione e regolamento subordinati che attuino il GDPR che può essere applicato.

1.5 **Soggetto cui si riferiscono i dati personali** ha il significato attribuito nella legislazione sulla protezione dei dati.

1.6 **Violazione dei dati personali:** una violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati.

1.7 Tutti gli altri termini indicati con la lettera maiuscola avranno il significato attribuito nella Legislazione sulla protezione dei dati o nell'MSA.

2. ELABORAZIONE DATI

2.1 Le parti riconoscono e accettano che per quanto riguarda il trattamento dei dati personali, il Cliente è il Responsabile del trattamento e Mapp è l'Incaricato del trattamento.

2.2 Le parti rispettano i rispettivi obblighi ai sensi delle leggi e dei regolamenti sulla protezione dei dati. Ciascuna delle parti, nel suo utilizzo dei Servizi Mapp, tratterà i Dati personali solo in conformità con i requisiti delle leggi e dei regolamenti sulla protezione dei dati.

2.3 Le istruzioni del Cliente per il trattamento dei dati personali devono essere conformi alle leggi e ai regolamenti sulla protezione dei dati. Mapp comunicherà immediatamente al Cliente se, a suo parere, un'istruzione da parte del Cliente viola leggi e regolamenti sulla protezione dei dati.

2.4 Mapp elabora i Dati personali solo per conto e in conformità con le istruzioni documentate del Cliente ai fini di (i) elaborazione in conformità con MSA; (ii) elaborazione avviata dagli Utenti nel loro utilizzo dei Servizi; (iii) elaborazione per conformarsi ad altre istruzioni ragionevoli documentate fornite dal Cliente; (iv) tutela della

riservatezza, integrità e disponibilità dei Dati Personali e dei Servizi in conformità con questo accordo; e (v) raccolta di statistiche non identificabili.

2.5 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 DIRITTI DELLE PERSONE INTERESSATE

3.1 Mapp, nella misura consentita dalla legge, notifica tempestivamente al Cliente se Mapp riceve una richiesta da una persona interessata per esercitare uno o più diritti dei soggetti cui si riferiscono i dati personali come definito nel capitolo III GDPR (33-36) ("**Richiesta DSR"**).

3.2 Tenendo conto della natura del Trattamento, 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 DSR ai sensi delle Leggi e Regolamenti sulla Protezione dei Dati.

3.3 Nella misura in cui il Cliente, nel suo utilizzo dei Servizi, non ha la capacità di inviare una Richiesta DSR, Mapp dovrà, su richiesta del Cliente, fare ogni sforzo commercialmente ragionevole per aiutare il Cliente a rispondere a tale Richiesta DSR, nella misura in cui Mapp sia legalmente autorizzato a farlo e la risposta a tale richiesta DSR sia 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 Mapp.

4. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Mapp fornirà un'assistenza ragionevole al Cliente con eventuali valutazioni d'impatto sulla protezione dei dati e consultazioni preventive con un'autorità di vigilanza, richieste ai sensi delle leggi e dei regolamenti sulla protezione dei dati, in ciascun caso esclusivamente in relazione al trattamento dei dati personali, e tenendo conto della natura dell'elaborazione e le informazioni disponibili per Mapp.

5. COMUNICAZIONE DELLA VIOLAZIONE DEI DATI PERSONALI

5.1 Mapp dà tempestiva comunicazione al Cliente di una violazione dei dati personali dopo esserne venuto a conoscenza. Mapp fornirà al Cliente informazioni sufficienti per consentire al Cliente di adempiere a qualsiasi obbligo di notifica all'Autorità di Vigilanza della Violazione dei dati personali e/o di comunicare la Violazione dei dati personali agli interessati ai sensi delle Leggi sulla protezione dei dati.

5.2 Mapp dovrà compiere ogni ragionevole sforzo per identificare la causa di una violazione dei dati personali e prendere quei provvedimenti che ritiene necessari e ragionevoli al fine di rimediare alla causa di tale Incidente di Dati del Cliente nella misura in cui il risanamento rientra nel ragionevole controllo di Mapp.

5.3 Gli obblighi di questo documento non si applicano agli incidenti causati dal Cliente.

6. SUB-CONTRATTO

6.1 Gli Affiliati di Mapp e gli altri subincaricati utilizzati da Mapp per fornire i propri servizi contrattuali, compreso il loro ruolo e ambito di sub-contratto e l'area geografica di sub-contratto sono pubblicati nell'elenco dei subincaricati di Mapp disponibile su richiesta e/o accessibile all'indirizzo www.mapp.com/contracts. Tali subincaricati devono essere concordati e accettati dal Cliente. Firmando questo DPA, il Cliente accetta l'elenco dei subincaricati qui allegato come Appendice 3 e con la presente autorizza Mapp a trasferire i Dati Personali agli Affiliati di Mapp elencati e/o ad altri subincaricati in ubicazioni al di fuori dell'Area Economica Europea, come ragionevolmente richiesto a fornire supporto, realizzare progetti tecnici o eseguire altri tipi di servizi nell'ambito dell'MSA, a condizione che, se il Cliente è incorporato nell'UE, sia: (i) tali ubicazioni siano riconosciute dalla Commissione europea in quanto forniscono un'adeguata protezione dei dati; o (ii) Mapp abbia eseguito le clausole contrattuali standard dell'UE con tali affiliati e/o altri subincaricati.

6.2 Mapp ha stipulato un accordo scritto con ciascun subincaricato contenente obblighi di protezione dei dati non meno protettivi rispetto a quelli in questo DPA in relazione alla protezione dei Dati personali nella misura applicabile alla natura dei Servizi forniti da tale subincaricato.

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

6.4 Mapp anticipa la necessità di modificare o aggiungere un subincaricato Mapp che deve notificare al Cliente qualsiasi cambiamento nel subincaricato e il Cliente avrà il diritto di contraddire qualsiasi cambiamento entro un ragionevole lasso di tempo. Laddove il Cliente non dovesse contraddire tale cambiamento entro tale periodo di tempo, si riterrà che il Cliente abbia acconsentito a tale cambiamento. Laddove esista una ragione di concreta rilevanza per tale contraddizione, e in mancanza di una risoluzione amichevole della questione dalle parti, il Cliente avrà il diritto di rescindere il DPA. Mapp garantirà che ogni nuovo subincaricato sia considerato secondo le stesse norme applicabili ai subincaricati precedentemente concordati.

7. SICUREZZA

Tenuto conto delle conoscenze tecniche, dei costi dell'esecuzione 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 del cliente), la riservatezza e l'integrità dei dati personali, come stabilito nell'allegato sulla sicurezza di Mapp (Appendice 2) per questo DPA. Mapp controlla regolarmente la conformità con queste misure. Mapp non ridurrà materialmente la sicurezza complessiva dei Servizi durante la durata dell'MSA. Mapp limiterà l'accesso ai Dati personali ai propri dipendenti o subincaricati 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 o equivalenti di Mapp o che siano soggetti ad un obbligo legale di riservatezza appropriato. La politica di sicurezza dell'informazione di Mapp può essere fornita su richiesta. Il cliente preferisce ulteriori dettagli relativi a questa sezione.

8. CANCELLAZIONE O RETTIFICA DEI DATI PERSONALI

8.1 Mapp cancellerà i Dati Personali al termine/scadenza dell'MSA come specificato nell'MSA o su richiesta ragionevole del Cliente entro 30 giorni e assicurerà che i dati cancellati non siano recuperabili. Mapp può conservare i Dati personali nella misura richiesta dalle leggi applicabili e solo nella misura e per il periodo richiesto dalle leggi applicabili e sempre a condizione che Mapp garantisca la riservatezza di tutti tali Dati Personali e garantisca 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 questa sezione 8.

8.3 Mapp restituirà i Dati personali al Cliente secondo la procedura e i tempi specificati nell'MSA.

9. AUDIT E ISPEZIONI

9.1 Mapp mette a disposizione del Cliente tutte le informazioni necessarie a dimostrare la conformità con questo DPA e deve consentire e contribuire a verifiche da parte del Cliente o di un revisore di terze parti 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 in merito alle pratiche e alle politiche di protezione dei dati e della sicurezza delle informazioni di Mapp.

9.2 Il cliente o un revisore di terze parti incaricato dal Cliente può, a spese del Cliente e non più di una volta l'anno, eseguire un'ispezione in loco delle pratiche e delle politiche di protezione dei dati e della sicurezza delle informazioni di Mapp con una comunicazione scritta ragionevolmente, con almeno dieci giorni lavorativi di anticipo. L'ispezione deve svolgersi in un solo giorno durante il normale orario di lavoro di Mapp su un programma concordato che riduca al minimo l'impatto dell'audit sulle operazioni di Mapp. Il cliente o un 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 a più utenti in condivisione (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 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 a questo DPA e tutti i DPA tra Affiliate e Mapp, sia in contratto, illecito civile o qualsiasi altra teoria di responsabilità, è soggetta alla sezione di limitazione di responsabilità concordata ai sensi dell'MSA 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 all'MSA e ad ogni DPA si applica in forma aggregata per tutte le rivendicazioni ai sensi sia dell'MSA sia di tutti i DPA stabiliti ai sensi di questo accordo.

10.3 Laddove un interessato asserisca qualsivoglia diritto nei confronti di una parte di questo DPA ai sensi dell'art. 82 GDPR, l'altra parte sosterrà nella difesa contro tali richieste, ove possibile.

Appendice 1: Persone e categorie cui si riferiscono i dati personali
Appendice 2: Allegato sulla sicurezza
Appendice 3: Elenco degli affiliati e dei subcontraenti di Mapp

RESPONSABILE DEL TRATTAMENTO		**INCARICATO DEL TRATTAMENTO**	
Firma:		Firma:	
Nome stampato, titolo:		Nome stampato, titolo:	Steven Warren, CEO
Data:		Data:	

APPENDICE 1: PERSONE E CATEGORIE CUI SI RIFERISCONO I DATI PERSONALI

Persone cui si riferiscono i dati personali. I dati personali trattati riguardano le seguenti categorie di interessati:

- Clienti del cliente,
- Probabili clienti 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 elaborati o utilizzati.	Le misure sono progettate, applicate e monitorate in conformità con la normativa 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'autentica 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 la normativa 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”. 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 alla normativa 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 recensioni di accesso specifiche dell'applicazione.

	- I sistemi di archiviazione applicano la crittografia a livello di filesystem o oggetto usando AES-256 (o equivalente). - 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 alla normativa 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. - Gli ambienti di sviluppo, test e produzione sono separati. - 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 alla normativa 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 (si applica a Mapp Acquire). - 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 alla normativa 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 (elaborati 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 alla normativa 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 alla normativa 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 alla normativa 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 con la normativa 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 alla normativa 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	**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 alla normativa 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. I nostri servizi software sono altamente personalizzabili. Le opzioni per la configurazione sono disponibili nella rispettiva guida in linea. - I clienti rimangono responsabili per l'uso legale e rispettoso della privacy dei servizi software di Mapp. Inoltre, si applica la Politica sull'utilizzo accettabile: 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 alla normativa ISO 27001:2013, in particolare A.8.3.2, A.11.2.7, A.13.2.1 e A.18.1.1. Queste includono: - Mappare i dati dei processi solo in base alle istruzioni del Cliente, ovvero in base a 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 DIGITALI E SUBCONTRAENTI DI MAPP

Subincaricato	Luogo di elaborazione (e garanzie legali, se al di fuori del SEE)	Scopo
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*	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 Certificate ai sensi dello UE-USA Privacy Shield)	Interno: supporto e servizi, ricerca e sviluppo [solo Mapp Empower]
Aprimo / MEMO Marketing Operations Philippines Inc	Filippine (clausole contrattuali standard)	Interno: supporto e servizi
Aprimo Australia Pty Ltd	Australia (clausole contrattuali standard)	Interno: supporto
Pythian Group Inc.	Canada (decisione sull'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)	Esterno: infrastruttura del centro di dati [solo Mapp Empower]
Google, LLC.	Elaborazione principale e archiviazione dei dati in Belgio. Raccolta globalmente distribuita tecnicamente necessaria a causa della natura dei Servizi (Clausole contrattuali standard)	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)	Esterno: SMS [Mapp Engage, opzionale]
R & D Communications Srl	Italia	Esterno: SMS [Mapp Engage, opzionale]
Mitto AG	Germania e Svizzera (decisione sull'adeguatezza)	Esterno: SMS [Mapp Engage, opzionale]
WebTrekk GmbH	Germania e Italia	Interno: Mapp Intelligence
SL Webtrekk Analytics	Spagna	Interno: Mapp Intelligence

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

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