MOMIT SRL
Viale Enrico Forlanini 23 – 20134 - Milano

DATA PROCESSING AGREEMENT

ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI

Il presente Accordo relativo alla protezione dei dati personali è concluso tra il "Fornitore", che verrà considerato nella sua figura di "Responsabile" o "SubResponsabile del trattamento dei dati personali" e il "Committente", nella sua figura di "Titolare" o a propria volta "Responsabile" del trattamento dei dati personali.

Per "Fornitore" si intende la società MOMIT S.R.L., con sede legale in Viale Enrico Forlanini, 23, 20134 Milano, P.IVA / C.F IT07634600964. Per "Committente" si intende il soggetto indicato nel contratto quale Committente o Cliente.

Congiuntamente tali soggetti possono essere anche indicati come "le Parti".

PREMESSA

Tra le Parti è in essere un rapporto contrattuale che contempla fornitura di servizi.

Per le "definizioni" di tali servizi si rimanda integralmente alle Condizioni di Generali di Fornitura, presenti all'indirizzo www.momit.eu/condizioni-generali-di-servizio/ da intendersi qui richiamate.

Trattamento dei dati personali ai fini dell'esecuzione del Contratto.

Il trattamento dei dati personali comunicati dal Committente a Momit S.r.L. ai fini dell'esecuzione del presente Contratto e della successiva erogazione del Servizio, avverrà in conformità al D.lgs. 196/2003 (con le modifiche apportate dal D.lgs. 101/2018) e al Regolamento europeo n. 679/2016, all'informativa privacy rinvenibile sul sito del Fornitore all'indirizzo www.momit.eu/privacy .

Momit S.R.L., per le sole fasi di raccolta, trattamento e gestione dei dati necessarie ai fini dell'erogazione dei Servizi e dell'erogazione delle prestazioni contrattuali, è da qualificarsi quale Titolare del trattamento in conformità alle prescrizioni di cui al Regolamento Europeo n. 679/2016 ed alle indicazioni e Linee Guida delle Autorità di controllo.

Il Committente garantisce, con riferimento ai dati del proprio personale trattati nell'esecuzione delle prestazioni necessarie all'esecuzione del contratto, di aver preventivamente fornito loro le informazioni di cui all'art. 13 del Regolamento Europeo già citato. Resta comunque inteso che il Committente si pone, rispetto a tali dati, quale Titolare autonomo del trattamento, assumendo tutti gli obblighi e le responsabilità ad esso connesse.

Il Committente garantisce nello stesso senso e con le medesime modalità e conseguenze, di avere preventivamente fornito le necessarie informazioni e se del caso ottenuto il necessario consenso al trattamento dei dati personali dei

terzi per ogni fase dell'utilizzo dei servizi di cui al contratto, manlevando Momit S.R.L. da ogni contestazione, pretesa o altro che dovesse provenire da terzi soggetti in riferimento a tali ipotesi di trattamento.

Nell'esecuzione di tale contratto il Fornitore - Responsabile - ha accesso e, in ragione del caso concreto, dovrà trattare, secondo quanto definito dal Reg. Europeo n. 679/2016 all'art. 4, 1, 2), il c.d. GDPR, una serie di dati personali per conto del Committente, il quale, rispetto a tali dati, ricopre il ruolo di Titolare del trattamento (ovvero a propria volta di Responsabile, e in tale ipotesi il ruolo e la veste di Momit S.R.L. saranno quelli del SubResponsabile), secondo quanto meglio definito nel GDPR.

Alla luce di quanto sopra, le parti hanno convenuto di stipulare il presente Accordo per soddisfare gli obblighi imposti al Fornitore ai sensi del GDPR ovvero delle altre norme in materia di privacy e protezione dei dati personali applicabili.

Il Committente ha verificato e ritenuto adeguate e sufficienti le competenze e conoscenze tecniche del Fornitore in relazione alle finalità e alle modalità di trattamento dei dati personali, alle misure tecniche e organizzative da adottare a tutela della riservatezza, completezza ed integrità dei dati personali, secondo quanto indicato dalla normativa italiana ed europea e ha ritenuto che il Fornitore possieda requisiti di affidabilità idonei a garantire il rispetto delle disposizioni normative in materia.

Sulla base delle referenze e competenze verificate dal Committente in termini di proprietà, risorse umane, attrezzature ed esperienza nella gestione di servizi analoghi a quelli di cui al Contratto in essere nonché degli impegni contrattuali assunti dal Fornitore in tema di rispetto della normativa applicabile in materia di protezione dei dati personali, il Committente ha condotto una positiva valutazione della idoneità e qualificazione del Fornitore e intende affidare a quest'ultimo alcune operazioni di trattamento dei dati personali ai sensi e per gli effetti di cui all'art. 28 del GDPR. Tutto quanto sopra premesso, le Parti convengono come segue.

DEFINIZIONI

Nel presente Atto i termini e le espressioni che seguono avranno il seguente significato.

Contratto di fornitura	Indica il rapporto intercorrente tra il Committente e il Fornitore
Dati Personali	Sarà interpretato in conformità alla Legislazione in materia di Protezione dei Dati Personali e includerà, a titolo puramente esemplificativo e non esaustivo, tutti i dati nella misura in cui siano oggetto di trattamento da parte del Fornitore, o per suo conto, sulla base del Contratto, come ad esempio i dati anagrafici e i dati di contatto e qualsiasi informazione

	riguardante una persona fisica identificata o identificabile. Un elenco dei dati personali trattati è riportato all'Appendice A al presente documento
Decisione di Adeguatezza	Indica una decisione della Commissione Europea ai sensi dell'articolo 45, n. 3, del GDPR, affinché le leggi di un certo paese garantiscano un adeguato livello di protezione, come previsto dalla Legislazione in materia di Protezione dei Dati Personali
Istruzioni	Indica le istruzioni scritte impartite dal Committente, riportate nel Contratto e/o nel presente Accordo o negli Allegati a quest'ultimo
Legislazione in materia di Protezione dei Dati Personali	Indica il GDPR ed eventuali normative e/o decreti legislativi di adeguamento del quadro normativo nazionale alle disposizioni del GDPR (es: d.lgs. 196/2003, d.lgs. 101/2018) ed emanati ai sensi dello stesso o in vigenza della normativa previgente al GDPR, nonché ogni provvedimento vincolante emanato dalle autorità di controllo competenti in materia (ad esempio il Garante per la protezione dei dati personali) nonché dal Comitato europeo per la protezione dei dati emanate anche prima del 25 maggio 2018 ma che ne conservi efficacia vincolante.
Particolari Categorie di Dati Personali (dati Particolari)	Indica qualunque informazione idonea a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale di una persona fisica
Personale del Fornitore	Indica le persone fisiche, identificate, autorizzate e istruite a trattare i Dati Personali sotto l'autorità del Fornitore, ivi inclusi, a titolo esemplificativo e non esaustivo: i lavoratori dipendenti, autonomi o interinali, gli stagisti, i dirigenti, i rappresentanti e qualsiasi soggetto che presti attività lavorativa a favore del Fornitore, con esclusione del personale dei Responsabili Ulteriori del trattamento
Richiesta di esercizio dei diritti	Indica una richiesta di accesso di un interessato o di una richiesta di cancellazione o correzione dei Dati Personali o una richiesta di esercizio di uno degli altri diritti previsti dal GDPR

Responsabile Ulteriore del trattamento	Indica qualunque subappaltatore o altro soggetto terzo a cui Fornitore abbia subappaltato, affidato, o di cui si intenda avvalere per l'esecuzione di tutte o di parte delle operazioni di trattamento dei Dati Personali, svolte su incarico del Committente ai fini della prestazione dei Servizi
Violazione della sicurezza dei Dati Personali	Indica la violazione di 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, conservati o comunque trattati occorsa sui sistemi gestiti da Fornitore o comunque sui quali Fornitore possa esercitare un controllo
Interessato, Trattamento, Trasferimento, Titolare del trattamento, Responsabile del trattamento e Misure tecnico – organizzative adeguate	Tali termini saranno interpretati in conformità alla Legislazione in materia di Protezione dei Dati Personali. Si veda l'art. 4 del Regolamento Europeo 679/2016

2. RUOLO DELLE PARTI

2. Le Parti convengono che il Fornitore svolge operazioni di trattamento di Dati Personali per conto del Committente. Il Fornitore ha nominato un Responsabile per la Protezione dei Dati (RPD - DPO, Data Protection Officer), domiciliato c/o la sede della Momit Srl in viale Forlanini 23, 20134 Milano che può essere contattato al seguente indirizzo: privacy@momit.it.

3. OGGETTO

3. Con la sottoscrizione del Contratto, il Fornitore agirà, sulla base del presente Accordo, quale Responsabile del trattamento, in relazione alle operazioni di trattamento dei Dati Personali conferiti dal Committente, ai soli fini dell'esecuzione del Contratto e della prestazione dei Servizi.

I compiti assegnati al Fornitore sono esclusivamente quelli resi necessari dalle attività connesse all'esecuzione del Contratto e alla prestazione dei Servizi.

4. OBBLIGHI DEL FORNITORE

4. Il Fornitore si obbliga in favore del Committente a:

- trattare i Dati Personali allo scopo di adempiere al Contratto di Fornitura dei Servizi Cloud, nel rispetto del presente accordo e secondo le istruzioni ricevute (in modalità documentata), di volta in volta, dal Committente;
- non esercitare esso stesso il controllo, né trasferire o pretendere di trasferire, il controllo dei Dati Personali a terzi, salvo che sulla base di specifiche istruzioni ricevute dal Committente;
- non elaborare o utilizzare i Dati Personali per scopi diversi da quelli indicati dal Committente;
- non trattare i Dati Personali trattati per conto del Committente per propri scopi o comunque includere i Dati Personali in alcun prodotto o servizio offerto o da offrire a terzi;
- adempiere regolarmente alle prescrizioni e conservare la documentazione relativa ai trattamenti per come prescritto dalle norme in materia di protezione dei dati personali.

Al fine di garantire che le istruzioni del Committente, in relazione a qualsiasi Dato Personale da trattare per conto del Committente, possano essere eseguite secondo quanto previsto dal presente Accordo, il Fornitore dovrà predisporre processi e misure tecniche appropriate. In particolare dovrà fare in modo che:

- eventuali richieste da parte di singoli utenti effettuate al Committente, o comunque l'esercizio da parte degli Utenti dei diritti in tema di privacy, in relazione ai propri Dati personali, di volta in volta, possano essere soddisfatte nel rispetto di quanto previsto dalla normativa in materia di protezione dei dati personali;
- i Dati Personali degli Utenti possano essere aggiornati, modificati o corretti su semplice richiesta del Committente;
- su richiesta del Committente l'accesso ai dati personali possa essere annullato o bloccato.

Il Fornitore dovrà fornire al Committente la cooperazione, l'assistenza e le informazioni che il Committente possa ragionevolmente richiedere per consentirgli di adempiere ai propri obblighi ai sensi della normativa in materia di protezione dei dati personali e dovrà conformarsi alle direttive o alle decisioni del Garante Privacy e cooperare con lo stesso, in un tempo tale da permettere al Committente di rispettare eventuali termini a quest'ultimo imposti.

Prima di procedere a ciascun trattamento per conto del Committente il Fornitore provvederà ad informare quest'ultimo:

- se una richiesta e/o un'istruzione avanzata dal Committente, ad opinione del Fornitore, possa confliggere con la normativa in materia di protezione dei dati personali;
- se sia impossibile per il Fornitore agire secondo quanto richiesto dal Committente poiché la richiesta esporrebbe il Fornitore ad una violazione della normativa in materia di protezione dei dati personali.

Nel caso di cui al punto precedente, il Fornitore avrà facoltà di non soddisfare la richiesta e/o le istruzioni del Committente e di sospendere l'adempimento del presente contratto nonché del Contratto di fornitura software e servizi senza che da ciò possa discendere responsabilità alcuna.

Ove, invece, la richiesta del Committente possa essere soddisfatta ma sia necessaria una variazione e/o integrazione dei prodotti e/o servizi resi in virtù del Contratto di fornitura, il Fornitore comunicherà tempestivamente, tale possibilità al Committente con il relativo costo. Il Committente dovrà accettare (con il relativo costo) ovvero rifiutare la variazione entro cinque giorni dalla comunicazione; nel caso non accettasse, il Fornitore potrà astenersi dal soddisfare la richiesta di Trattamento del Committente senza che da ciò possa derivarne in capo allo stesso alcuna responsabilità.

Precisato quanto sopra, resta fermo tra le Parti che il Fornitore non svolge consulenza in tema di Privacy, trattamento dei dati personali o normative in materia di protezione degli stessi al Committente né è o potrà essere ritenuto responsabile per la individuazione delle fattispecie di legge applicabili al Committente e alla sua attività commerciale e/o industriale; tantomeno il Fornitore potrà essere ritenuto responsabile della conformità delle attività svolte dal Committente nello sfruttamento dei Prodotti e dei servizi di cui al Contratto.

Il Fornitore garantisce che l'accesso ai Dati Personali e il loro trattamento sia effettuato solo in base al principio di stretta necessità, provvedendo a individuare e istruire per iscritto, anche ai fini dell'art. 32 del GDPR, il proprio personale preposto al trattamento dei Dati Personali e assicurando che sia soggetto a idonei vincoli di riservatezza. I soggetti autorizzati al trattamento, in relazione allo svolgimento delle attività sopra descritte, saranno specificamente assegnati al trattamento dal Fornitore dando loro le istruzioni necessarie e rendendoli edotti delle modalità convenute e di quelle prescritte e dal Regolamento UE 2016/679.

Il Fornitore si impegna altresì a non comunicare, divulgare o consentire l'accesso a soggetti terzi (siano esse persone fisiche o giuridiche) ai Dati Personali senza previa autorizzazione scritta rilasciata dal Committente, salvo che tale comunicazione sia dovuta per legge o su ordine delle autorità competenti; in tale ultima ipotesi il Fornitore informerà preventivamente e per iscritto Committente, salvo che ciò sia vietato dalla legge o dalle autorità competenti;

Il Fornitore si impegna ad adottare tutte le misure richieste ai sensi dell'articolo 32 del Regolamento UE 2016/679 in relazione al trattamento dei Dati Personali che possa essere effettuato dal proprio personale anche in qualità di amministratore di sistema, in linea con i principi indicati nei provvedimenti del Garante per la protezione dei dati personali di cui al 27 novembre 2008 e ad apprestare ogni altra misura idonea a consentire la rilevazione di anomalie negli accessi e nelle operazioni di trattamento sui Dati Personali nonché a mantenere il controllo sull'operato degli amministratori di sistema come previsto dalla normativa vigente.

Il Fornitore applicherà le misure indicate nel Contratto, nelle Condizioni Generali di servizio, nelle procedure adottate secondo lo standard ISO 27001 e meglio descritte nell'Appendice A del presente Accordo.

Tenuto conto della natura e della tipologia dei trattamenti demandati, il Fornitore si impegna a informare il Committente, entro 12 ore dal momento in cui ne sia venuto a conoscenza, di qualsiasi Violazione della sicurezza dei Dati Personali o rischio di Violazione della sicurezza dei Dati Personali di cui il Fornitore venga a conoscenza, inviando una comunicazione contenga:

i) la data e l'ora in cui si è verificata la Violazione dei Dati Personali;

ii) una descrizione dettagliata di come e quando si è verificata la Violazione di sicurezza dei Dati Personali, incluse le categorie e il numero approssimativo di Interessati e di Dati Personali colpiti e le misure adottate per evitare o mitigare gli effetti di tale Violazione;

iii) le probabili conseguenze della Violazione dei Dati Personali;

iv) una descrizione dettagliata di come e quando è stata identificata la Violazione di sicurezza dei Dati Personali;

v) i nomi e i dati di contatto del proprio RPD, o i recapiti di una persona di riferimento di Fornitore da cui è possibile ottenere maggiori informazioni e,

vi) non appena possibile, ogni altra informazione raccolta o resa disponibili, nonché ogni altra informazione che possa essere ragionevolmente richiesta da Committente relativamente alla Violazione di sicurezza dei Dati Personali.

5. OBBLIGHI DEL COMMITTENTE

5. Il Committente dichiara e garantisce, ad ogni buon conto, che il Trattamento dei Dati Personali che egli andrà ad effettuare e per il quale utilizzerà la collaborazione del Fornitore, sarà in ogni caso legittimo e che, pertanto non utilizzerà i prodotti e i servizi di cui al Contratto di fornitura software e servizi per finalità che comportino la violazione delle normative in materia di protezione dei dati personali né di alcuna altra normativa applicabile.

6. OBBLIGHI DI ENTRAMBE LE PARTI

6. Le parti si impegnano a considerare informazioni confidenziali, ai sensi di quanto previsto dal Contratto, le informazioni attinenti le eventuali Violazioni della sicurezza dei Dati Personali. Entrambe si impegnano a informare senza indugio l'altra parte in caso di qualsiasi richiesta di informazione, attività ispettiva o provvedimento delle autorità aventi ad oggetto i Dati Personali in modo che possano collaborare al fine di dare riscontro alle autorità.

7. RESPONSABILI ULTERIORI DEL TRATTAMENTO

7. Il Fornitore potrà esternalizzare a terzi operazioni di trattamento di Dati Personali nel rispetto delle norme in materia di protezione dei dati personali.

Il presente atto costituisce, in ogni caso, autorizzazione generale alla subfornitura.

Resta inteso che in tali ipotesi il Fornitore provvederà a:

- provvedere affinché il Responsabile Ulteriore, prima di iniziare il trattamento dei Dati Personali *i)* sottoscriva un contratto con Fornitore mediante il quale il Responsabile Ulteriore assuma obblighi in materia di protezione dei dati personali analoghi a quelli di cui al presente Atto e *ii)* fornisca adeguate garanzie per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento dei Dati Personali soddisfi i requisiti previsti dalla Legislazione in materia di Protezione dei Dati Personali; copia di tale contratto potrà essere trasmessa al Committente, su richiesta di quest'ultimo;
- vigilare e monitorare con la dovuta diligenza sul rispetto degli obblighi in materia di protezione dei dati personali da parte del Responsabile Ulteriore, fermo restando che ai sensi dell'art. 28 (4) del GDPR, qualora il Responsabile Ulteriore ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Fornitore rimane pienamente responsabile nei confronti del Committente per l'adempimento degli obblighi del Responsabile Ulteriore.
- almeno 15 (quindici) giorni prima della data di avvio delle operazioni di trattamento dei Dati Personali da parte del Responsabile Ulteriore del Trattamento informa il Cliente dell'affidamento al terzo (nonché dei dati identificativi del terzo, della sua ubicazione – _ed eventualmente, dell'ubicazione dei server sui quali saranno conservati i dati, se applicabile - e delle attività affidate) mediante invio di Email di notifica o altro mezzo ritenuto idoneo dal Fornitore. Il Cliente potrà recedere dal Contratto entro 15 (quindici) giorni dal ricevimento della

comunicazione, fermo restando l'obbligo di corrispondere al Fornitore gli importi dovuti alla data di cessazione del Contratto.

8. LIMITAZIONE AL TRASFERIMENTO DEI DATI AL DI FUORI DELLO SPAZIO ECONOMICO EUROPEO (SEE)

8. I Dati Personali non potranno essere trasferiti al di fuori dello Spazio Economico Europeo ("SEE") senza accordo con il Committente.

Se, ai fini della conservazione o del trattamento dei Dati Personali da parte di un Responsabile Ulteriore del trattamento, è necessario effettuare il trasferimento dei Dati Personali fuori dallo SEE in un paese che non gode di una decisione di adeguatezza da parte della Commissione Europea ai sensi dell'art. 45 del GDPR, il Fornitore:

- farà in modo che il Responsabile Ulteriore del trattamento stipuli le clausole contrattuali tipo previste nella Decisione della Commissione europea 2010/87/UE del 5 febbraio 2010, per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi (le "Clausole Contrattuali Tipo") o loro equivalente, se modificate nel tempo. Copia delle Clausole Contrattuali Tipo sottoscritte dal Fornitore per conto del Committente saranno rese disponibili al Committente. Con il presente Accordo il Committente conferisce espressamente mandato al Fornitore a sottoscrivere le Clausole Contrattuali Tipo con i Responsabili Ulteriori del Trattamento riportati nei relativi DPA. Qualora Titolare del trattamento sia l'Utente Finale, il Committente si impegna a informare l'Utente Finale di tale trasferimento e dichiara che l'autorizzazione ad avvalersi del Responsabile Ulteriore del Trattamento situato fuori dallo SEE equivale al mandato di cui sopra. In aggiunta e/o in alternativa
- In aggiunta e/o in alternativa potrà proporre a quest'ultimo altre modalità di trasferimento dei Dati Personali conformi a quanto previsto dalla Legislazione in materia di Protezione dei Dati Personali.

9. MISURE DI SICUREZZA

9. Con riferimento alle operazioni di trattamento dei Dati Personali necessarie ai fini dell'esecuzione del Contratto e della prestazione dei Servizi, il Fornitore si obbliga ad adottare e mantenere Misure tecnico-organizzative idonee ad assicurare la massima riservatezza dei Dati Personali e a garantire un livello di sicurezza adeguato ai rischi, idoneo a prevenire i rischi di distruzione, perdita, anche accidentale, dei Dati Personali nonché di accesso non autorizzato o trattamento illecito e a far sì che tali misure siano conformi alle misure idonee a garantire il rispetto di quanto previsto

dall'art. 32 del GDPR. Il Fornitore si impegna a verificare regolarmente l'idoneità delle misure adottate e ad aggiornarle. Si veda nel dettaglio quanto previsto al punto 4 "Obblighi del Fornitore".

10. CONTROLLI - DURATA

10. Il Fornitore riconosce che il Committente potrà effettuare verifiche delle operazioni di trattamento di Dati Personali mediante richieste di informazioni e/o documenti che dovranno essere tempestivamente forniti.

Il presente accordo ha la medesima durata del contratto in essere tra le parti parti oltre al tempo necessario per l'eliminazione dei dati presenti al termine del servizio.

11. DISPOSIZIONI IN MATERIA DI CANCELLAZIONE E RESTITUZIONE DEI DATI

11. Alla cessazione del Servizio, per qualunque causa intervenuta, il Fornitore cesserà ogni trattamento dei Dati Personali e provvederà alla cancellazione dei Dati Personali (ivi incluse eventuali copie) dai sistemi del Fornitore o da quelli su cui lo stesso abbia controllo entro il termine previsto nel Contratto, tranne il caso in cui la conservazione dei dati da parte del Fornitore sia necessaria al fine di assolvere ad una disposizione di legge italiana o europea. Distruggerà eventuali Dati Personali conservati in formato cartaceo in suo possesso, tranne il caso in cui la conservazione dei dati da parte del Fornitore sia necessaria ai fini del rispetto di norme di legge italiane o europee e manterrà a disposizione del Cliente i Dati Personali per l'estrazione per 15 giorni successivi alla cessazione del Contratto.

Fermo restando quanto altrimenti previsto nel presente Accordo, il Committente riconosce di poter estrarre i Dati Personali, alla cessazione del Servizio, nei modi convenuti nel Contratto e conviene che è sua responsabilità provvedere all'estrazione totale o parziale dei soli Dati Personali che ritenga utile conservare e che tale estrazione dovrà essere effettuata prima della scadenza del termine di cui al punto precedente.

12. DISPOSIZIONI VARIE

12. Il presente Accordo potrà essere modificato dal Fornitore dandone comunicazione scritta (anche via e-mail o con l'ausilio di programmi informatici) al Committente. In tal caso, il Committente avrà il diritto di recedere dal Contratto con comunicazione scritta inviata al Fornitore a mezzo PEC all'indirizzo momit@legalmail.it nel termine di 15 giorni dal ricevimento della comunicazione del Fornitore. In mancanza di esercizio del diritto di recesso da parte del Committente, nei termini e nei modi sopra indicati, le modifiche al presente Accordo si intenderanno da questi definitivamente conosciute e accettate e diverranno definitivamente efficaci e vincolanti.

In caso di conflitto tra le previsioni del presente Accordo e quanto previsto nel Contratto per la prestazione dei Servizi, o in documenti del Committente non espressamente accettati dal Fornitore in deroga al presente Accordo e ai rispettivi DPA – Condizioni Speciali, prevarrà quanto previsto nel presente Accordo e nelle clausole dei relativi DPA Condizioni Particolari.

APPENDICE A

MISURE DI SICUREZZA

In aggiunta a quanto convenuto in Contratto e nelle Condizioni Generali di Fornitura e a quanto sopra indicato il Fornitore si impegna ad applicare anche le seguenti misure tecniche e organizzative di sicurezza.

MISURE DI SICUREZZA ORGANIZZATIVE	DETTAGLIO
Controllo degli accessi al Datacenter	Sono previste misure volte a prevenire l'accesso fisico non autorizzato ai locali e agli impianti in cui sono trattati i dati personali oggetto del contratto. In particolare sono adottati sistemi e misure per il controllo e la registrazione degli accessi, l'apertura e la chiusura delle porte, sistemi di sorveglianza e videosorveglianza, sistemi di allarme.
Controllo degli accessi logici ai sistemi ed ai dati personali	Il Fornitore definisce i profili di accesso nel rispetto del least privilege necessari all'esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti. Sono adottate specifiche procedure relative alla creazione, gestione cambio e modifica di username e password ed adottati regolamenti e procedure interne volte ad assicurare la sicurezza di reti, applicazioni, dispositivi, database e piattaforme. Ove possibile vengono utilizzate password monouso e autenticazione a due fattori per garantire l'univocità dell'accesso.
Controllo della diffusione dei dati durante la trasmissione	Al fine di evitare l'accesso non autorizzato, la modifica o l'eliminazione dei Dati Personali durante la loro trasmissione e garantire che tutte le trasmissioni siano sicure e registrate, vengono adottate misure che includono la pseudonimizzazione e la crittografia mediante canali e strumenti valutati dal Fornitore come sicuri. Si assicura il divieto assoluto di utilizzo di dispositivi di memorizzazione portatili (a mero titolo di esempio: chiavette usb, mobile phone, cloud non autorizzati), Come procedura interna si garantisce per ogni trasferimento la creazione di record cronologici (log di accesso), oltre che la pseudonimizzazione e la cifratura dei dati.

Controllo delle attività, della disponibilità, separazione e archiviazione	Al fine di garantire che il trattamento dei Dati Personali avvenga rigorosamente in conformità alle istruzioni fornite dal Titolare, sono adottate misure che includono la redazione delle istruzioni al personale autorizzato in modo univoco, procedure per il monitoraggio dell'esecuzione dell'Accordo e dei servizi di cui al Contratto, selezione dei dipendenti e dei collaboratori autorizzati e loro supervisione. Sono adottate particolari misure organizzative al fine di garantire la conservazione e la disponibilità delle informazioni trattate in virtù del contratto, anche in relazione all'archiviazione delle stesse. Ulteriori misure sono adottate al fine di consentire che i dati personali raccolti per finalità diverse siano trattati separatamente (a titolo esemplificativo: separazione logica dei database, separazione degli ambienti informatici di produzione e test, pseudonimizzazione, laddove richiesta, dei dati personali).
D.P.I.A.	In conformità agli artt. 35 e 36 del GDPR, al documento WP 248 – Linee guida sulla valutazione d'impatto nella protezione dei dati adottate dal Gruppo di lavoro ex art. 29 nonché all'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018 (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018), il Fornitore ha predisposto una propria metodologia per l'analisi e la valutazione dei trattamenti che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, presentino un rischio elevato per i diritti e le libertà delle persone fisiche allo scopo di procedere con la valutazione dell'impatto sulla protezione dei dati personali prima di iniziare il trattamento. La DPIA viene realizzata per alcuni trattamenti ma il sistema di analisi dei rischi e delle misure di mitigazione degli stessi per la sicurezza delle informazioni è stata effettuata in conformità con quanto richiesto dall'annex A della ISO/IEC 27001:2013
Incident management	Il Fornitore ha realizzato una specifica procedura di Incident Management e un Businnes Continuity Plan allo scopo di garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile, garantendo il mantenimento dei livelli migliori di servizio.
Data Breach	Il Fornitore ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali al Cliente.

Formazione	Il Fornitore eroga periodicamente ai propri dipendenti e a tutto il personale coinvolto nelle attività di trattamento, corsi di formazione sulla corretta gestione dei dati personali e sugli strumenti implementati per a loro gestione.

MISURE DI SICUREZZA TECNICHE	DETTAGLIO
Linee di comunicazione	I dati personali sono protetti contro il rischio d'intrusione di cui all'art. 615-quinquies del codice penale mediante sistemi di Intrusion Detection & Prevention e mantenuti aggiornati in relazione alle migliori tecnologie disponibili. Sono adottati dal Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile.
Protezione da Virus	I sistemi sono protetti da strumenti Antivirus aggiornati in tempo reale.
Protezione da malware e ransomware	I sistemi sono protetti contro il rischio di intrusione e dell'azione di programmi mediante l'attivazione di idonei strumenti elettronici aggiornati con cadenza periodica.
Credenziali di autenticazione	I sistemi sono configurati con modalità idonee a consentirne l'accesso unicamente a soggetti dotati di credenziali di autenticazione che ne consentono la loro univoca identificazione.
Password	Relativamente alle caratteristiche di base ovvero, obbligo di modifica al primo accesso, lunghezza minima, assenza di elementi riconducibili agevolmente al soggetto, regole di complessità, scadenza, history, valutazione contestuale della robustezza, visualizzazione e archiviazione, la password è gestita conformemente alle best practice. Ai soggetti ai quali sono attribuite le credenziali sono fornite puntuali istruzioni in relazione alle modalità da adottare per assicurarne la segretezza.
Logging	I sistemi sono configurati con modalità che consentono il tracciamento degli accessi da parte delle diverse tipologie di utenze e protetti da adeguate misure di sicurezza che ne garantiscono l'integrità.
Backup & Restore	Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati. In base agli accordi contrattuali è posto in uso un piano di continuità operativa integrato, ove necessario oppure un piano di disaster recovery; essi garantiscono

	la disponibilità e l'accesso ai sistemi anche nel caso di eventi negativi di portata rilevante che dovessero perdurare nel tempo.
A.d.S.	Relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di log management finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il monitoraggio. L'operato degli Amministratori di Sistema è sottoposto ad attività di verifica in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti, come prescritto anche dall'Autorità Garante con il provvedimento del 27 novembre 2008.
Data Center	L'accesso fisico al Data Center è limitato ai soli soggetti autorizzati. Per il dettaglio delle misure di sicurezza adottate con riferimento ai servizi di data center erogati nonché per i Responsabili Ulteriori (Sub Responsabili) individuati si fa rinvio alle misure di sicurezza indicate e descritte nel seguente documento: Infrastruttura_datacenter_v2_it-IT. Scaricabile all'indirizzo https://momit.ryo.cloud sezione documenti previa autenticazione.