Accordo sul Trattamento dei Dati Personali

ai sensi di quanto previsto dal Regolamento UE 2016/679

Tra

Società di Progetto Brebemi S.p.A.

Iscr. Registro Imprese di Brescia - Cod. Fisc. e P.IVA 03514010986

Sede legale: Via Somalia, 2/4 - 25126 Brescia

di seguito, il "Titolare del trattamento" o "Brebemi"

E

[Iscr. Registro Imprese - Denominazione sociale]

[C.F./P.IVA]

[Sede legale]

di seguito, il "Responsabile del trattamento" o il "Fornitore"

Data del presente Accordo sul trattamento dei dati:	……../……../…….
Durata del presente Accordo sul trattamento dei dati:	Il presente Accordo sul trattamento dei dati permarrà in vigore per tutta la durata del contratto principale di prestazione servizi (il "Contratto", di cui *infra*), come eventualmente prorogato o rinnovato, fino al completo adempimento di tutti gli obblighi relativi alla privacy e alla protezione dei dati derivanti da detto Contratto e dal presente Accordo sul trattamento dei dati
Contratto principale a cui il presente Accordo sul trattamento dei dati è accessorio (di seguito, il "Contratto")	Contratto prot. n…… del ……. avente ad oggetto l'affidamento del servizio di ……
Nome e dati di contatto del Responsabile della protezione dei dati di Brebemi	Avv. Antonio Comes Email: privacy@brebemi.it
Nome e dati di contatto del Responsabile della protezione dei dati del Fornitore	…… ……

Allegati:	Allegato I: Categorie di dati e attività affidate al sub-Responsabile del trattamento Allegato II: ulteriori sub-responsabili autorizzati Allegato III: misure di sicurezza tecniche e organizzative Allegato IV: Modulo di richiesta di autorizzazione di sub-Responsabili

1. Oggetto

L'oggetto del presente Accordo sul trattamento dei dati è quello di disciplinare gli obblighi del Fornitore in qualità di Responsabile del trattamento dei dati nei confronti del Titolare del trattamento nell'ambito della fornitura dei servizi prestati a quest'ultimo ai sensi del **Contratto**.

Nell'**Allegato I** al presente Accordo sul trattamento dei dati si descrivono:

- Attività di trattamento dei dati affidate al Responsabile del trattamento
- Categorie di dati
- Categorie di interessati
- Finalità

In caso di contrasto tra le previsioni del **Contratto** e quelle del presente Accordo sul trattamento dei dati su qualsiasi aspetto relativo al trattamento dei dati personali, prevarranno le disposizioni del presente documento.

2. Definizioni

VIOLAZIONE DEI DATI PERSONALI: ogni violazione di sicurezza che comporta accidentalmente o in modo illecito o intenzionale la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso, dei dati personali trasmessi, conservati o comunque trattati.

DATO PERSONALE: qualsiasi informazione riguardante una persona fisica identificata (per esempio: nome e cognome, fotografia, immagine) o identificabile (voce, targa, indirizzo IP, eccetera).

INTERESSATO: la persona fisica cui si riferiscono i dati personali o, se del caso, il suo rappresentante (legale o volontario).

MISURE E ORGANIZZAZIONE DI SICUREZZA: assumono il significato di cui alla Sezione 8.

NORMATIVA SULLA PROTEZIONE DEI DATI PERSONALI: qualsiasi norma legale o regolamentare avente per oggetto il trattamento dei dati personali, incluso, a titolo esemplificativo e non limitativo, il Regolamento (UE) 679/2016 ("GDPR"), le normative applicabili a settori specifici e le raccomandazioni e linee guida eventualmente emesse dalle autorità per la protezione dei dati

TRATTAMENTO (O ATTIVITÀ DI TRATTAMENTO): qualsiasi operazione o insieme di operazioni applicate a dati personali, come la raccolta, la registrazione, la conservazione, l'adattamento o la modifica, la consultazione, l'uso, la cancellazione, la limitazione o la distruzione dei dati personali, nonché la trasmissione di dati

personali mediante comunicazione o qualsiasi altra forma di messa a disposizione, interconnessione o trasferimento di dati personali.

3. Trattamento conforme alle istruzioni del Titolare del trattamento

Obblighi del Responsabile del trattamento:

i. Elaborare i dati personali unicamente in conformità alle disposizioni del presente Accordo sul trattamento dei dati, alle istruzioni del Titolare del trattamento e ai requisiti applicabili in materia di protezione dei dati.

ii. Informare immediatamente il Titolare del trattamento se ritiene che alcuna delle istruzioni impartite da quest'ultimo possa contravvenire ai requisiti in materia di protezione dei dati.

iii. Fornire, a richiesta del Titolare del trattamento, ogni genere di informazione e documentazione eventualmente necessarie per assicurare il rispetto dei requisiti in materia di protezione dei dati e per dimostrare la conformità a detti requisiti da parte dei fornitori che trattano i dati personali per conto del Titolare del trattamento, in particolare, a titolo esemplificativo e non esaustivo, per le seguenti finalità:
   - Per soddisfare i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita.
   - Per la corretta tenuta dei registri delle attività di trattamento.
   - Per la conduzione integrale e adeguata delle valutazioni d'impatto sulla protezione dei dati, se richieste.
   - Per la cooperazione e le notifiche alle autorità per la protezione dei dati.
   - Per assistere il Titolare del trattamento nell’esercizio o la difesa di un diritto in sede giudiziaria in caso di violazione dei requisiti in materia di protezione dei dati eventualmente imputabile a quest'ultimo come risultato del trattamento realizzato dal Responsabile del trattamento.
   - Per assicurare la sicurezza nel trattamento dei dati.
   - Per la gestione dei diritti degli interessati.
   - Eccetera.

iv. Nominare un rappresentante, debitamente qualificato in materia di protezione dei dati personali, e autorizzato dal Responsabile del trattamento a ricevere istruzioni dal Titolare del trattamento. Qualora il Titolare del trattamento impartisca istruzioni orali, è tenuto a confermarle per iscritto il più presto possibile.

4. Luogo di trattamento e trasferimento di dati personali al di fuori dello Spazio Economico Europeo

4.1. Il trattamento dei dati personali da parte del Responsabile del trattamento deve essere effettuato presso i locali specificati nell'Allegato I del presente Accordo sul trattamento dei dati, salvo diversamente autorizzato per iscritto dal Titolare del trattamento.

4.2. Il Responsabile del trattamento non ha facoltà di trasferire al di fuori dello Spazio Economico Europeo ("SEE") i dati personali trattati per conto del Titolare del trattamento senza la previa autorizzazione scritta di quest'ultimo e previo adempimento dei seguenti requisiti:

- Il Fornitore si impegna a formalizzare gli opportuni **accordi contrattuali idonei** a garantire un livello di protezione della privacy e dei dati personali analogo a quello imposto dai requisiti in materia di protezione dei dati o approvati dalle autorità di controllo interessate, **come nel caso delle clausole contrattuali tipo adottate dalla Commissione europea.**
- Il Responsabile del trattamento è tenuto a condurre un'**analisi documentata del quadro normativo del paese di destinazione**, per verificare che sussistano le misure di sicurezza e i meccanismi sufficienti a garantire il rispetto degli obblighi contrattuali di cui alla sezione precedente.
- Qualora il risultato dell'analisi di tale quadro normativo non sia soddisfacente, il Responsabile del trattamento è tenuto a informarne il Titolare del trattamento, il quale può rifiutare l'autorizzazione o richiedere l'attuazione di **misure di sicurezza e meccanismi supplementari** per mitigare il rischio e l'impatto, quali, tra le altre:

    - cifratura dei dati custoditi o in transito
    - anonimizzazione
    - separazione dei dati mediante partizione
    - pseudonimizzazione
    - minimizzazione dei dati
    - localizzazione di determinati dati
    - maggiori diritti per gli interessati
    - obblighi contrattuali aggiuntivi (come obblighi informativi, o l'obbligo di fare opposizione a eventuali ingiunzioni delle pubbliche autorità dei paesi di destinazione)

4.3. L'analisi documentata, nonché le misure di sicurezza e i meccanismi supplementari, devono essere comunicati dal Responsabile del trattamento al Titolare del trattamento con un preavviso minimo di trenta (30) giorni di calendario dalla data in cui il Responsabile del trattamento intende rendere effettivo il trasferimento dei dati trattati per conto del Titolare del trattamento, per consentire a quest'ultimo di valutare adeguatamente la richiesta di autorizzazione.

4.4. Ai sensi delle disposizioni della presente clausola e di quella successiva (Sub-responsabili), anche la mera divulgazione di dati personali con qualsiasi mezzo (ad es. oralmente o concedendo, diritti di sola lettura, anche in caso impossibilità assoluta di manipolazione, eccetera) deve intendersi come “trasferimento di dati personali”.

5. Sub-responsabili del trattamento

5.1. Il Responsabile del trattamento non ha facoltà di designare alcun sub-responsabile del trattamento all’infuori di quelli approvati nell'**Allegato II** del presente Accordo sul trattamento dei dati, salvo previa autorizzazione scritta del Titolare del trattamento, che il Responsabile del trattamento deve richiedere nel formato e con il contenuto specificati nell'**Allegato IV**.

Al momento di identificare i suoi sub-responsabili del trattamento e di richiedere l'autorizzazione corrispondente, il Responsabile del trattamento deve prendere in considerazione, *nella misura in cui detti sub-responsabili realizzino qualche*

tipo di trattamento dei dati personali per conto del Titolare del trattamento, i seguenti tipi di fornitori:

- Fornitori di servizi di housing (centro dati, indicandone l'ubicazione)
- Fornitori di servizi di hosting (hosting, indicando da dove opera il fornitore)
- Fornitori di servizi IT (sviluppo, mantenimento, supporto, controlli di sicurezza, ecc.)
- Fornitori di altri servizi (non informatici) che devono accedere ai dati personali o comunque realizzarne il trattamento.

5.2. Il Responsabile del trattamento è tenuto a eseguire una due diligence sui subappaltatori da selezionare, nonché sulle garanzie da essi fornite riguardanti la conformità ai requisiti in materia di protezione dei dati.

5.3. Il Responsabile del trattamento si impegna a stipulare i necessari accordi e contratti scritti con i subappaltatori comunque intervenienti nel trattamento dei dati personali per conto del Titolare del trattamento (sub-responsabili del trattamento), vincolandoli all'ottemperanza degli stessi obblighi del presente Accordo sul trattamento dei dati e dei requisiti applicabili in materia di protezione dei dati imposti al Responsabile del trattamento, quali, a titolo esemplificativo e non limitativo, l'obbligo di riservatezza, l'obbligo del possesso di idonee qualifiche professionali, l'obbligo di impartire corsi di formazione ai dipendenti del sub-responsabile del trattamento, nonché l'obbligo di notifica immediata di violazioni dei dati personali (da comunicare direttamente al Titolare del trattamento), oppure conferendo al Titolare del trattamento gli stessi diritti nei confronti del sub-responsabile del trattamento riguardo alla verifica dell'adempimento degli obblighi derivanti dal presente Accordo sul trattamento dei dati e dai requisiti in materia di protezione dei dati vantati dal Titolare del trattamento nei confronti del Responsabile del trattamento (inclusi diritti di informazione, audit e ispezione).

5.4. Il Titolare del trattamento si riserva il diritto di richiedere in qualsiasi momento al Responsabile del trattamento copia degli accordi sulla protezione dei dati stipulati con i rispettivi sub-responsabili coinvolti nel trattamento dei dati personali per conto del Titolare del trattamento. Il Titolare del trattamento si impegna da parte sua a mantenere riservati i dati dettagliati e i segreti commerciali contenuti in tali accordi.

5.5. Le disposizioni della Sezione 4 del presente Accordo sul trattamento dei dati si applicano anche nel caso in cui il Responsabile del trattamento intenda designare un sub-responsabile e coinvolgerlo nel trattamento dei dati che realizza per conto del Titolare del trattamento, e ciò comporti un trasferimento di dati al di fuori dello Spazio Economico Europeo nei termini descritti in detta clausola.

5.6. In caso di subappalto da parte di un sub-responsabile del trattamento di attività che comportano il trattamento di dati per conto del Titolare del trattamento, è obbligatorio ottenere la previa autorizzazione scritta di quest'ultimo.

5.7. Fatte salve le disposizioni della presente clausola, il Responsabile del trattamento risponde legalmente e contrattualmente nei confronti del Titolare del trattamento per ogni atto ed omissione relativi al trattamento dei dati personali affidato ai sub-responsabili operanti sotto la sua designazione.

6. Diritti di proprietà intellettuale e obblighi di riservatezza

6.1. Tutti i dati personali oggetto di trattamento da parte del Responsabile del trattamento e dei suoi sub-responsabili per conto del Titolare del trattamento rimangono comunque di proprietà di quest'ultimo. Il Responsabile del trattamento si impegna a cedere e a trasferire al Titolare del trattamento qualsiasi diritto, titolo o interesse sui dati personali trattati per conto di quest'ultimo, nonché tutte le informazioni che possa ottenere o possano corrispondergli in relazione a tali dati.

6.2. Il Responsabile del trattamento si impegna a mantenere segreti e riservati i dati personali affidatigli in conformità al presente Accordo sul trattamento dei dati, impegnandosi altresì a:

- Coinvolgere nel trattamento dei dati personali solo i dipendenti che necessitano effettivamente la conoscenza di tali dati per la prestazione dei servizi oggetto del Contratto.
- Impartire ai propri dipendenti corsi di formazione sui requisiti in materia di protezione dei dati e sui loro obblighi ai sensi del presente Accordo sul trattamento dei dati, nonché sui loro doveri di segretezza e riservatezza.
- A richiesta del Titolare del trattamento, Responsabile del trattamento è tenuto a imporre ai propri dipendenti e ai dipendenti dei suoi sub-responsabili, la stipula degli opportuni patti di riservatezza, che devono rimanere a disposizione del Titolare del trattamento.

6.3. Tutte le parti coinvolte nella prestazione dei servizi oggetto del Contratto si impegnano a mantenere strettamente confidenziali tutte le informazioni a cui accedono come conseguenza della negoziazione, della stipula e dell'esecuzione del Contratto che non siano già di dominio pubblico, come segreti commerciali, know-how, eccetera, e si impegnano a non conservare, divulgare o fare qualsiasi altro uso delle informazioni loro fornite o divulgate per la prestazione dei Servizi.

6.4. Il Responsabile del trattamento è tenuto a informare il Titolare del trattamento di qualsiasi procedura di audit, accertamento o ispezione eventualmente avviata sui dati personali trattati per conto di quest'ultimo dal Responsabile del trattamento o dai suoi sub-responsabili, e a informare i responsabili di tali azioni che il trattamento di tali dati viene eseguito per conto e sotto le istruzioni del Titolare del trattamento.

7. Obbligo di distruzione o restituzione dei dati

7.1. Il Responsabile del trattamento si impegna a procedere al trattamento dei dati personali per tutto il tempo necessario per espletare le attività di trattamento oggetto del presente Accordo sul trattamento dei dati. Una volta concluse dette attività, il Responsabile del trattamento si impegna a distruggere o a restituire al Titolare del trattamento (come richiesto da quest'ultimo) tutti i dati, i documenti, i prodotti risultanti dal trattamento e gli insiemi di dati relativi al presente Accordo sul trattamento dei dati:

- Qualora il Titolare del trattamento opti per la restituzione dei dati, il Responsabile del trattamento è tenuto a procedervi utilizzando un formato strutturato, di uso comune e leggibile elettronicamente.

- Nel caso in cui il Titolare del trattamento opti per la distruzione o la cancellazione delle informazioni, il Responsabile del trattamento è tenuto a fornirgli un registro attestante l'effettiva eliminazione dei dati.

La mancanza di istruzioni specifiche del Titolare del trattamento in nessun caso deve intendersi come un'estensione della legittimità del trattamento per il Responsabile del trattamento, il quale, in assenza di istruzioni al riguardo, è comunque tenuto a richiederle proattivamente.

7.2. Il Responsabile del trattamento non ha facoltà di realizzare copie o duplicati dei dati personali senza la previa autorizzazione scritta del Titolare del trattamento, ad eccezione delle copie di backup e di ripristino eventualmente necessarie per motivi di sicurezza per garantire l'integrità e la disponibilità dei dati personali.

7.3. Le disposizioni della presente clausola non devono intendersi come ostative al diritto del Responsabile del trattamento di conservare le informazioni e la documentazione idonee a dimostrare la conformità del trattamento dei dati personali per tutta la durata dell'Accordo sul trattamento dei dati.

Una volta concluse le attività di trattamento di cui al presente Accordo, il Responsabile del trattamento ha facoltà di conservare le informazioni e la documentazione a tal fine necessarie, debitamente bloccate e protette, a disposizione unicamente dei giudici, dei tribunali e delle pubbliche amministrazioni, con obbligo di distruggerle completamente una volta decorsi i termini di prescrizione degli obblighi contrattuali, legali, amministrativi e, se del caso, penali eventualmente derivanti dal trattamento dei dati personali.

8. Misure di sicurezza tecniche e organizzative

Il Responsabile del trattamento si impegna a progettare, sviluppare e implementare in modo efficiente le misure di sicurezza tecniche e organizzative specificate nell'Allegato III al presente Accordo sul trattamento dei dati.

9. Registro delle attività di trattamento

Il Responsabile del trattamento si impegna a tenere un registro delle attività di trattamento realizzate per conto terzi, il cui contenuto minimo deve stabilirsi in conformità ai requisiti applicabili in materia di protezione dei dati.

10. Violazione dei dati personali

10.1 Nel caso in cui il Responsabile del trattamento rilevi alcun evento suscettibile di compromettere la riservatezza, l'integrità e/o la disponibilità dati personali trattati per conto del Titolare del trattamento, è tenuto a informane immediatamente quest'ultimo, senza ingiustificato ritardo e comunque entro le dodici (12) ore successive alla sua rilevazione, all'indirizzo privacy@brebemi.it, indicando nell'oggetto: *"Notifica di possibile incidente di sicurezza o violazione dei dati personali"*

10.2. La notificazione deve contenere le seguenti informazioni:

a. Denominazione della società Titolare del trattamento
b. Persona che effettua la segnalazione e dati di contatto in caso di necessità di ulteriori informazioni
c. Data e ora in cui si viene a conoscenza dell'incidente di sicurezza/violazione dei dati personali
d. Data di inizio dell'incidente di sicurezza/violazione dei dati personali, se nota
e. Data di risoluzione o di contenimento dell'incidente di sicurezza/violazione dei dati personali, se nota
f. Indicazione della tipologia di incidente di sicurezza/violazione dei dati personali: derivante dal trattamento automatizzato (informatico) o meno
g. Origine dell'incidente di sicurezza: interna (nell'ambito dell'organizzazione); esterna (estranea all'organizzazione) o sconosciuta
h. Natura dell'incidente di sicurezza: dolosa/intenzionale, o accidentale
i. Tipologia dell'incidente di sicurezza/violazione dei dati personali: Se l'incidente di sicurezza o violazione dei dati personali è suscettibile di compromettere la riservatezza e/o l'integrità e/o la disponibilità dei dati personali
j. Categorie di dati personali coinvolti (vedasi tabella)
k. Numero esatto o approssimativo di interessati
l. Numero esatto o approssimativo di registrazioni dei dati personali
m. Categorie di interessati (vedasi tabella)
n. Possibili conseguenze per gli interessati (vedasi tabella)
o. Misure di sicurezza preventive in essere prima dell'incidente di sicurezza/violazione dei dati personali
p. Misure correttive implementate a seguito dell'incidente di sicurezza/violazione dei dati personali per mitigarne gli effetti negativi e prevenirne la reiterazione

TABELLA	
Categorie di dati personali	☐ Dati generici ☐ Credenziali di accesso o di identificazione ☐ Dati di contatto ☐ Carta d'identità, permesso di soggiorno o passaporto ☐ Dati economico-finanziari ☐ Dati di localizzazione ☐ Dati su condanne penali e reati ☐ Convinzioni religiose o filosofiche ☐ Stato di salute ☐ Affiliazione sindacale ☐ Dati genetici ☐ Opinioni politiche ☐ Vita sessuale ☐ Dati biometrici (immagine facciale o dati dattiloscopici) ☐ Altri (specificare) ☐ Sconosciuti
Categorie di interessati	☐ Candidati/aspiranti a posto di lavoro ☐ Dipendenti ☐ Ex dipendenti ☐ Stagisti e personale iterino ☐ Fornitori (persona fisica) ☐ Amministratori e Dirigenti ☐ Clienti ☐ Utenti di social network

	☐ Visitatori dei locali di Brebemi ☐ Persone fisiche vulnerabili (minori, anziani o invalidi) ☐ Altri (specificare)
Possibili conseguenze per gli interessati	☐ Divulgazione a terzi/diffusione su Internet ☐ Arricchimento di altre banche dati ☐ Uso dei dati per finalità differenti da quelle consentite ☐ Dati alterati, resi inservibili o irrecuperabili ☐ Dati alterati e utilizzati per finalità diverse da quelle consentite ☐ Impossibilità della prestazione di un servizio agli interessati ☐ Deterioro delle condizioni di prestazione di un servizio agli interessati ☐ Perdita di controllo sui propri dati personali ☐ Usurpazione d'identità ☐ Re-identificazione non autorizzata ☐ Danni reputazionali ☐ Limitazione dei diritti dell'interessato ☐ Frode ☐ Violazione della riservatezza di dati tutelati dal segreto professionale ☐ Discriminazione ☐ Perdite economiche ☐ Sconosciute ☐ Altre (specificare)

10.2 Il Responsabile del trattamento si impegna a collaborare con il Titolare del trattamento fornendo le informazioni richieste da quest'ultimo per la gestione dell'incidente di sicurezza o violazione dei dati personali, per la valutazione del rischio che detto incidente di sicurezza o violazione dei dati personali rappresenta per gli interessati, e per la notifica alle autorità e agli interessati in caso di obbligo informativo.

10.3 Il Responsabile del trattamento si impegna a condurre, per conto proprio e a proprie spese, un'analisi forense e un audit di sicurezza qualora l'incidente di sicurezza costituisca una violazione dei dati personali trattati per conto del Titolare del trattamento, oppure riguardi le risorse informatiche in cui si realizza il trattamento dei dati personali o che ne permettono l'accesso, dovendo riferire al Titolare del trattamento i relativi risultati e le azioni correttive e preventive da attuare per evitarne la reiterazione.

10.4. Qualora l'incidente di sicurezza o violazione dei dati personali si verifichi all'interno dello stabilimento del Responsabile del trattamento o dei suoi sub-responsabili, il Responsabile del trattamento, a proprie spese, è tenuto a:

a. Effettuare le notifiche di obbligatorio adempimento alle autorità per la protezione dei dati e agli interessati con le forme, i contenuti e nei termini stabiliti dal Titolare del trattamento, in conformità ai requisiti applicabili in materia di protezione dei dati. Tali notifiche devono essere effettuate a nome e per conto del Titolare del trattamento e in ogni momento in stretta conformità alle sue istruzioni.

b. Prestare servizi di supporto e contenimento nonché ogni altra ragionevole assistenza agli interessati, direttamente o tramite terzi, qualora sia così richiesto: (i) dai requisiti in materia di protezione dei dati applicabili al

trattamento; (ii) dalle autorità per protezione dei dati personali; (iii) dalle disposizioni convenute tra le parti.

11. Esercizio dei diritti degli interessati in materia di protezione dei dati

11.1. Il Responsabile del trattamento ha facoltà di rettificare, cancellare o limitare il trattamento dei dati personali degli interessati dietro istruzioni del Titolare del trattamento.

11.2. Nel caso in cui il Responsabile del trattamento venga a conoscenza di errori o imprecisioni nei dati personali trattati per conto del Titolare del trattamento, deve informarne immediatamente quest'ultimo e modificare tali errori e imprecisioni su richiesta scritta dello stesso.

11.3. Nel caso in cui gli interessati si rivolgano direttamente al Responsabile del trattamento per l'esercizio dei loro diritti in materia di protezione dei dati, il Responsabile del trattamento è tenuto a deferire tali richieste direttamente al Titolare del trattamento per la gestione delle stesse, informando l'interessato di detto deferimento e della data in cui ha avuto luogo.

Il Responsabile del trattamento è tenuto ad attuare le misure e le procedure tecniche e organizzative per garantire che il Titolare del trattamento sia in grado di gestire le richieste di esercizio dei diritti degli interessati nei tempi e con le modalità richieste. Questo include, tra gli altri, i seguenti obblighi:

a) Avviare le procedure per fornire al Titolare del trattamento copia dei dati personali dell'interessato in formato strutturato, di uso comune e leggibile elettronicamente.
b) Fornire, a discrezione del Titolare del trattamento, ragionevole accesso ai sistemi del Responsabile del trattamento in cui i dati personali vengono trattati.
c) Fornire all'interessato le informazioni ragionevolmente esigibili o richiedibili sul trattamento dei dati personali realizzato dal Responsabile del trattamento per conto del Titolare del trattamento.

12. Audit

12.1. Il Responsabile del trattamento si impegna a consentire, e a vincolare contrattualmente i suoi sub-responsabili in tal senso, l'ispezione da parte dei revisori nominati dal Titolare del trattamento e, se del caso, dalle autorità competenti, sulle attività di trattamento realizzate dal Responsabile del trattamento e dai suoi sub-responsabili (inclusa l'effettiva attuazione di misure di sicurezza tecniche e operative), nonché la verifica della loro conformità alle istruzioni del Titolare del trattamento e ai requisiti applicabili in materia di protezione dei dati. Il Responsabile del trattamento si impegna inoltre a fornire a tali parti (e ai loro eventuali rappresentanti autorizzati) tutte le informazioni e i diritti di accesso (incluso l'accesso ai locali e alle banche dati).

12.2. Il Responsabile del trattamento si impegna a condurre periodicamente (almeno una volta all'anno) un audit interno di conformità avente per oggetto l'Accordo sul trattamento dei dati e i requisiti applicabili in materia di protezione dei dati, estendendolo ai suoi sub-responsabili, e a informare il Titolare del trattamento dell'esito di tale audit e del corrispondente piano d'azione per correggere

eventuali carenze riscontrate specificando: misure da adottare, responsabile, tempistiche e piano di follow-up.

12.3. In funzione dei risultati rilevati in occasione di tali ispezioni o audit (interni o esterni), il Responsabile del trattamento o i suoi sub-responsabili, a seconda dei casi, sono tenuti ad implementare, senza ingiustificato ritardo e a proprie spese, tutte le azioni correttive necessarie.

12.4. Nel caso in cui il Titolare del trattamento sia soggetto a ispezioni o accertamenti da parte delle autorità di controllo, il Responsabile del trattamento e i suoi sub-responsabili si impegnano a prestare al Titolare del trattamento il supporto e l'assistenza necessari nella misura in cui tali ispezioni o accertamenti coinvolgano il trattamento dei dati personali oggetto del presente Accordo sul trattamento dei dati.

Analogamente, nel caso in cui tali ispezioni o accertamenti riguardino il Responsabile del trattamento o i suoi sub-responsabili e abbiano per oggetto i dati personali trattati per conto del Titolare del trattamento, il Responsabile del trattamento deve informarne il Titolare del trattamento non appena ne venga a conoscenza e acconsentirvi in presenza di quest'ultimo se così richiesto.

13.Responsabilità del Fornitore

13.1 L'inadempimento da parte del Fornitore degli obblighi previsti dal presente documento comporterà il diritto di Brebemi di risolvere il presente Accordo e il relativo Contratto ai sensi e per gli effetti di quanto previsto dall'articolo 1456 del Codice Civile. Resta salva la facoltà per Brebemi di agire in giudizio per i danni causati dall'inadempimento del Fornitore.

13.2 Il Fornitore si impegna a manlevare e mantenere indenne Brebemi da ogni e qualsiasi danno o conseguenza pregiudizievole, costo, spesa (incluse eventuali spese legali), o onere che le predette Società dovessero subire in conseguenza o per effetto di inadempimento da parte del Fornitore dei suoi obblighi in materia di protezione dei dati personali o comunque derivanti da una Violazione dei Dati Personali subita dal Fornitore o da eventuali Sub-responsabili.

14.Clausole finali. Legge applicabile e foro competente

14.1 Resta inteso che il presente Accordo non comporta alcun diritto del Fornitore ad uno specifico compenso e/o indennità e/o rimborso - ulteriore rispetto a quanto previsto nel Contratto -.

14.2 Il presente Accordo è regolato dalla legge italiana.

14.3 Per qualsiasi controversia che dovesse sorgere in relazione al presente documento, è competente il Foro di Brescia.

15.Durata

Il presente Accordo sul trattamento permarrà in vigore per tutta la durata del contratto principale di prestazione servizi (il "Contratto", di cui alla prima pagina), come eventualmente prorogato o rinnovato, fino al completo adempimento di tutti gli obblighi relativi alla privacy e alla protezione dei dati derivanti da detto Contratto e dal presente Accordo sul trattamento dei dati.

[Titolare del trattamento]

Rappresentato da

Nome:

Carica:

Data:

Nome:

Carica:

Data:

[Responsabile del trattamento]

Rappresentato da

Nome:

Carica:

Data:

Nome:

Carica:

Data:

ALLEGATO I. DESCRIZIONE DEI DATI E DELLE ATTIVITÀ DI TRATTAMENTO

1. **Informazioni sui locali dai quali il Responsabile del trattamento realizza il trattamento dei dati personali**

.....
.....
.....

2. **Descrizione delle finalità e delle modalità del trattamento (si prega di includere una descrizione dettagliata della procedura o del flusso di lavoro, se disponibile)**

.....
.....
.....

3. **Attività di trattamento dei dati personali (si prega di selezionare tutte le risposte pertinenti)**

☐ Ricompilazione	☐ Registrazione	☐ Organizzazione
☐ Strutturazione	☐ Hosting/ Stoccaggio	☐ Adattamento o alterazione
☐ Ripristino	☐ Consultazione o lettura	☐ Uso
☐ Rivelazione	☐ Divulgazione	☐ Messa a disposizione
☐ Allineamento o combinazione	☐ Limitazione	☐ Cancellazione
☒ Distruzione	☐ Altri ….Fare clic o premere qui per inserire il testo…….	

4. **Categoria di interessati**

☐ Candidati/aspiranti a post di lavoro	☐ Fornitori (persona fisica)	☐ Visitatori dei locali di Brebemi
☐ Dipendenti	☐ Amministratori e Dirigenti	☐ Persone fisiche vulnerabi (minori, anziani o invalidi)
☐ Ex dipendenti	☐ Clienti	☐ Altri (specificare)…. Fare clic o premere qui per inserire il testo…..
☐ Stagisti e personale iterin	☐ Utenti di social network	

5. **Tipologia di dati personali**

☐ Dati generici	☐ Dati economico-finanziari	☐ Dati genetici
☐ Credenziali di accesso o c identificazione	☐ Dati di localizzazione	☐ Opinioni politiche
☐ Dati di contatto	☐ Dati su condanne penali e reati	☐ Vita sessuale
☐ Carta d'identità, permess di soggiorno o passaporto	☐ Convinzioni religiose o filosofiche	☐ Dati biometrici (immagine facciale o dati dattiloscopici)
☐ Affiliazione sindacale	☐ Stato di salute	

☒ Sconosciuti

☐ Altri (specificare)…. Fare clic o premere qui per inserire il testo……

ALLEGATO II. ULTERIORI SUB-RESPONSABILI AUTORIZZATI

Con la firma del presente Allegato, Brebemi autorizza i sub-responsabili incaricati dal Fornitore indicati di seguito (una tabella per ogni sub-responsabile autorizzato: è possibile raggruppare quelli che condividono le stesse informazioni nelle sezioni da d ad h).

a. Denominazione sociale del sub-responsabile del trattamento*
.....
b. Sede legale del sub-responsabile del trattamento*
.....
c. Locali o uffici del sub-responsabile presso i quali deve realizzarsi il trattamento dei dati*
.....
d. Finalità per cui il sub-responsabile deve realizzare il trattamento dei dati per conto del Titolare del trattamento*
.....
e. Attività di trattamento dei dati personali (vedasi attività applicabili al punto 5 dell'Allegato I) *
.....
f. Categorie di interessati (vedasi categorie applicabili al punto 6 dell'Allegato I)*
.....
g. Tipologie di dati personali (vedasi tipologie applicabili al punto 7 dell'Allegato I)*
.....
h. Categorie speciali di dati personali (se applicabili)*
.....
i. Persona preposta alla protezione dei dati o Responsabile della protezione dei dati del sub-responsabile del trattamento*
.....

ALLEGATO III. MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

Ambito di applicazione delle misure di sicurezza

1. Fornitori che realizzano il trattamento dei dati personali per conto di BREBEMI, nonché subappaltatori terzi che, previa autorizzazione di BREBEMI, possono essere incaricati dal Fornitore di eseguire una qualsiasi delle prestazioni necessarie per la fornitura del servizio appaltato da BREBEMI.
2. Sistemi d'informazione e risorse informatiche dei soggetti di cui sopra in cui si realizza il trattamento di informazioni riservate o di dati personali di BREBEMI o che ne permettono l'accesso, nella misura in cui risultino loro applicabili.

Il Fornitore e i subappaltatori che realizzano il trattamento di dati personali per conto di BREBEMI devono implementare le misure di sicurezza tecniche e organizzative sufficienti e idonee a garantire in ogni momento la riservatezza, l'integrità e la disponibilità di tali dati (custoditi o in transito) come esposte di seguito:

- Misure di sicurezza preventive, aggiornate in conformità allo stato della tecnica, volte a evitare violazioni della riservatezza, dell'integrità o della disponibilità dei dati personali.
- Controlli per rilevare eventi intenzionali o accidentali suscettibili di compromettere la riservatezza, l'integrità o la disponibilità dei dati personali.
- Procedure volte a garantire il rapido contenimento degli eventi rilevati, la loro analisi e risoluzione, nonché la loro notifica immediata a BREBEMI.

I. DEFINIZIONI

- **Evento di sicurezza:** evento o serie di eventi che, se considerati singolarmente e in mancanza di misure di sicurezza, potrebbero comportare la perdita di riservatezza, integrità o disponibilità di dati personali, ma che grazie alle misure di sicurezza sono privi di conseguenze o le cui conseguenze sono strettamente controllate. Un evento di sicurezza non produce necessariamente delle conseguenze dannose o avverse, normalmente è un segnale che le misure di sicurezza stanno funzionando.
- **Incidente di sicurezza:** evento o serie di eventi, accidentali o intenzionali, con una significativa probabilità di compromettere la riservatezza, l'integrità e/o la disponibilità dei dati personali il cui trattamento è realizzato direttamente da BREBEMI o da terzi (ad es. fornitori) per conto di quest'ultima.

II. MISURE DI SICUREZZA PREVENTIVE

III. Controllo degli accessi fisici

i. L'accesso alle strutture in cui il Fornitore o i suoi subappaltatori realizzano il trattamento dei dati personali per conto di BREBEMI deve essere limitato e protetto (ad es. tramite sistemi di controllo accessi e videosorveglianza).

ii. L'accesso alle strutture in cui si trovano risorse critiche come siti, permutatori intermedi e principali (IDF, MDF) o centri di elaborazione dati deve essere limitato agli utenti che hanno realmente necessità di accedervi:
   - tale necessità deve essere giustificata e documentata;
   - gli utenti autorizzati devono essere debitamente identificati;
   - è obbligatorio tenere un registro degli accessi a dette strutture per verificare chi, quando, quali compiti realizza e su quali risorse informatiche, al fine di poter di svolgere accertamenti su eventuali violazioni dei dati personali.

iii. Il Fornitore e i suoi subappaltatori che realizzano il trattamento dei dati personali per conto di BREBEMI devono stabilire delle politiche applicabili ai propri dipendenti per garantire che prendano le opportune precauzioni per proteggere i loro monitor dalla vista di qualsiasi persona non autorizzata, soprattutto quando prestano servizio fuori dei rispettivi locali. Laddove possibile, il Fornitore e i suoi subappaltatori devono fornire ai propri dipendenti dei filtri per la privacy per gli schermi.

IV. Controlli specifici per il trattamento non automatizzato dei dati personali (su supporto cartaceo).

Obblighi del Fornitore e dei suoi subappaltatori

i. Evitare la stampa di documentazione contenente dati personali oggetto del trattamento per conto di BREBEMI.

ii. Disporre di armadi o spazi idonei all'archiviazione (temporanea o permanente) dei documenti stampati che possono contenere dati personali di BREBEMI e che per la loro natura devono:
   - essere custoditi sottochiave;
   - essere riservati ai dipendenti che ne hanno realmente necessità per lo svolgimento delle loro mansioni.

iii. Stabilire politiche di "clean desk" per assicurare che i dati personali rimangano in ogni momento sotto la sorveglianza dell'utente autorizzato, e custoditi sottochiave quando tale dipendente è assente, anche temporaneamente, dal suo posto di lavoro.

iv. Garantire l'esistenza di copia fisica o digitalizzata dei dati personali oggetto del trattamento in supporto cartaceo e la possibilità di ripristino dell'integrità e della disponibilità delle informazioni in caso di necessità.

v. Adottare misure volte a impedire, in caso di trasferimento fisico della documentazione, l'accesso non autorizzato alle informazioni ivi contenute o la loro manipolazione, da parte di persone non autorizzate.

vi. Impartire formazione al personale in materia di misure di sicurezza applicabili a questo tipo di documentazione e sulla necessità di segnalare senza ingiustificato ritardo qualsiasi evento di cui si venga a conoscenza suscettibile di compromettere la riservatezza, l'integrità e/o la disponibilità delle informazioni.

vii. Verificare periodicamente l'adempimento di tali obblighi e documentare eventuali non conformità e relative azioni correttive.

I dati personali oggetto del trattamento non automatizzato (su supporto cartaceo) del Fornitore o dei suoi subappaltatori per conto di BREBEMI devono essere altresì protetti anche da accessi non autorizzati o da eventi suscettibili di comprometterne l'integrità o la disponibilità, al fine di assicurare che rimangano in ogni momento sotto la sorveglianza dell'utente autorizzato, e custoditi sottochiave quando tale dipendente è assente, anche temporaneamente, dal suo posto di lavoro (politiche di "clean desk").

V. Controllo degli accessi logici

Il Fornitore e i subappaltatori che realizzano il trattamento dei dati personali per conto di BREBEMI devono implementare dei meccanismi di accesso logico a reti, sistemi di informazione e restanti risorse informatiche in cui il Fornitore e i suoi subappaltatori realizzano il trattamento dei dati personali per conto di BREBEMI, meccanismi che devono essere regolati dai principi esposti di seguito:

i. Devono essere basati su profili e utenti.
ii. I diritti di accesso (locale o remoto) devono essere configurati secondo il principio del minimo privilegio ("PoLP").
iii. La creazione di profili di amministratore deve essere basata su criteri di necessità giustificati e documentati. Gli utenti con tali profili devono essere debitamente identificati.
iv. Devono stabilirsi delle limitazioni all'accesso a determinate categorie di siti web come: social network, siti di download e di streaming, indirizzi URL di spam, siti dai contenuti pornografici, violenti o incitanti all'odio e al razzismo, siti di armi, di giochi online e giochi d'azzardo, siti che promuovono hacking o attività illecite, siti di malware o non sicuri, siti di nudità e di biglietti virtuali d'auguri online, connessioni VPN, proxy, P2P, torrent e qualsiasi altra categoria ritenuta rilevante a tali effetti dal Fornitore o dal subappaltatore. Eventuali eccezioni a dette restrizioni devono essere debitamente giustificate, documentate e autorizzate.
v. I profili e gli utenti devono essere soggetti a regolari verifiche e aggiornamenti. In particolare, devono essere implementate delle procedure di creazione, cancellazione e modifica degli accessi logici degli utenti (ad es. in caso di licenziamento o cambio di mansioni), nonché di revisione e, se necessario, di rinnovo dei privilegi di accesso degli utenti autorizzati.
vi. Nel caso in cui richiedano la connessione all'Active Directory di BREBEMI, devono soddisfare i requisiti comunicati a tal fine da BREBEMI in conformità ai requisiti imposti dalla Direzione di Tecnologie dell'Informazione e Comunicazione (DTIC).
vii. Il Fornitore e i subappaltatori che devono garantire l'accesso remoto alle risorse informatiche che permettono l'accesso ai dati personali di BREBEMI o in cui ne viene realizzato il trattamento devono utilizzare canali di comunicazione e meccanismi di autenticazione sicuri, protetti mediante moderni protocolli e algoritmi di crittografia.
viii. Obblighi del Fornitore e dei subappaltatori che realizzano il trattamento di dati personali per conto di BREBEMI:
    - Stabilire dei meccanismi (politiche, procedure e, se possibile, controlli tecnici) per impedire al loro personale di utilizzare le risorse informatiche per scopi personali, limitando l'accesso a Internet e a qualsiasi sito web non autorizzato.
    - In caso di archiviazione su cloud, questa deve essere limitata esclusivamente a siti privati gestiti dal Fornitore e autorizzati da BREBEMI per l'hosting e il trattamento dei suoi dati personali.

VI. Autenticazione

Obblighi del Fornitore e dei subappaltatori che realizzano il trattamento di dati personali per conto di BREBEMI nei propri sistemi

i. Richiedere almeno username e password.
ii. Richiedere il cambio periodico delle password (almeno ogni 45 giorni).
iii. Monitorare gli accessi di utenti per rilevare eventuali deviazioni e attività insolite in relazione al funzionamento di ogni sistema e risorsa informatica (ad es. ripetuti tentativi di accesso falliti, accessi fuori del normale orario di lavoro, ecc.).
iv. Identificare gli account di utenti che richiedono un'autenticazione forte (amministratori di server, di telecomunicazioni e di sistemi) e considerare l'utilizzo di metodi alternativi di accesso con autenticazione a due fattori (token, biometrici o altri).

VII. Sicurezza delle reti

Le reti del Fornitore e dei subappaltatori che permettono l'accesso ai dati personali di BREBEMI o in cui ne viene realizzato il trattamento devono disporre delle misure di sicurezza elencate di seguito.

i. Devono essere segmentate in:
   - reti con contatto diretto con reti esterne (ad es. Internet);
   - reti private (utenti, server e amministrazione, interfacce dirette di server e dispositivi);
   - reti wireless (con accesso a risorse, dispositivi mobili e di ospiti) di BREBEMI e delle sue Unità di Business.
ii. Le comunicazioni in entrata e uscita tra i diversi segmenti devono essere protette con dispositivi di sicurezza come crittografia di canali, protocolli http, certificati di sicurezza aggiornati e non vulnerabili, firewall per applicazioni Web (WAF), firewall, applicazioni antimalware, applicazioni antispam, o almeno con liste di controllo accesso (ACL) sui router.
iii. Implementare controlli di rilevamento di minacce in rete come sistemi di prevenzione intrusioni (IPS), sistemi di rilevamento intrusioni (IDS), firewall, limitazioni di accesso come porte sicure, gestione delle identità (IM) e controllo accesso a reti (NAC), apparecchiature contro attacchi distribuiti di negazione del servizio (DDOS), apparecchiature di rilevamento e/o blocco di minacce persistenti avanzate (APT), ecc.
iv. Implementare avvisi e meccanismi per bloccare il traffico non autorizzato quando viene rilevato.
v. Definire le procedure di contenimento quando vengono rilevate delle minacce.
vi. Aggiornare i meccanismi di rilevamento e contenimento in conformità alle "lezioni apprese" e allo stato della tecnica.

VIII. Dati personali in transito

Per proteggere le informazioni riservate e i dati personali di BREBEMI in transito, il Fornitore e i suoi subappaltatori coinvolti nel trattamento di queste informazioni devono:

i. proteggere le informazioni riservate e i dati personali usando un medesimo insieme limitato di tecnologie e pratiche crittografiche;
ii. condurre revisioni periodiche sulle tecnologie, le pratiche e le procedure in atto per assicurare che le misure adottate siano aggiornate, sufficienti e appropriate.

IX. Riservatezza, integrità e disponibilità

Obblighi del Fornitore e dei suoi subappaltatori

i. Informare e impartire formazione ai propri dipendenti in materia di:
   - obblighi di riservatezza e di non divulgazione dei dati personali e rischi associati; revisione periodica delle procedure di revoca e modifica dei diritti di accesso degli utenti in caso di licenziamento e cambi di mansioni per garantirne l'adempimento; e
   - rischi associati a software malevolo
ii. Implementare misure per controllare, mitigare e minimizzare gli effetti negativi del software malevolo, nonché misure di protezione e di rilevamento di malware.
iii. Stabilire meccanismi e procedure per garantire che nessun software non autorizzato dal Fornitore o dai suoi subappaltatori venga installato dall'utente su dispositivi che permettono l'accesso ai dati personali di BREBEMI o in cui ne viene realizzato il trattamento, senza previo controllo di sicurezza.
iv. Pianificare la gestione della capacità delle risorse informatiche che supportano i servizi forniti a BREBEMI in modo da garantire il normale sviluppo degli stessi e la rapida risoluzione di qualsiasi incidente di sicurezza che possa compromettere tale capacità.

X. Separazione degli ambienti

Obblighi del Fornitore e dei suoi subappaltatori

i. Garantire la separazione di ambienti di produzione, test, copie di backup e di ripristino.
ii. Astenersi dalla conduzione di test con dati reali di BREBEMI, salvo sia indispensabile e previa realizzazione di una copia di backup e di ripristino. Il costo dell'utilizzo di dati fittizi o di soluzioni alternative agli sviluppi e/o test con dati reali non giustifica in nessun caso l'indispensabilità di questi ultimi.
iii. Garantire l'esistenza di processi e controlli per il passaggio da un ambiente all'altro (ad es. da ambiente di test ad ambiente di produzione).
iv. Registrare tutte le informazioni sull'ambiente di test (caratteristiche, informazioni sui dati del test, ecc. durante i test, e conservazione di queste informazioni per garantire la qualità dei risultati dei test e la replicabilità futura delle condizioni.
v. Implementare e documentare norme per lo sviluppo di software e di sistemi che permettono l'accesso ai dati personali di BREBEMI o in cui ne viene realizzato il trattamento (ad es. sicurezza dell'ambiente di sviluppo, linee guida per il linguaggio di programmazione da utilizzare per la codifica, requisiti di sicurezza in fase di progettazione, repository sicuri, ecc.)
vi. Includere i requisiti di sicurezza informatica nei requisiti di upgrading dei sistemi di informazione (sviluppo o acquisizione) che permettono l'accesso ai dati personali di BREBEMI o in cui ne viene realizzato il trattamento.

vii. Verificare periodicamente l'adempimento di tali requisiti.

XI. Configurazione e sviluppi di sistemi

Obblighi del Fornitore e dei suoi subappaltatori

i. Sviluppare e implementare processi per le modifiche di configurazione di sistemi e risorse informatiche che permettono l'accesso ai dati personali di BREBEMI o in cui ne viene realizzato il trattamento, che ne garantiscano la registrazione, revisione, autorizzazione e collaudo prima del loro impiego effettivo.
ii. Sviluppare e implementare dei processi per lo sviluppo di sistemi che permettono l'accesso ai dati personali di BREBEMI o in cui ne viene realizzato il trattamento, tenendo conto dei requisiti di sicurezza informatica e del principio di protezione dei dati personali fin dalla fase di progettazione, e che garantiscano la realizzazione di controlli sulle diverse versioni di software e il loro collaudo prima del loro impiego effettivo.
iii. Adottare una metodologia di sviluppo sicura focalizzata sul sistema in questione.

XII. Copie di back-up e di ripristino

Il Fornitore e i subappaltatori che realizzano il trattamento di dati personali per conto di BREBEMI devono realizzare periodicamente copie di back-up e di ripristino, che garantiscano l'integrità e la disponibilità delle informazioni e la continuità del servizio, nel rispetto dei requisiti elencati di seguito.

i. Esistenza di procedure documentate per la realizzazione di copie di back-up e di ripristino che devono soddisfare i seguenti requisiti:
    - includere le frequenze;
    - essere aggiornate in caso di modifica dei requisiti dell'attività aziendale, modifica di infrastrutture o sistemi che necessitano tali copie. Le procedure di realizzazione di copie di back-up devono essere allineate con il piano di contingenza e il piano di ripristino del Fornitore/subappaltatore;
    - definire il tipo di copia di back-up e relativi criteri di ritenzione (ad es. completo giornaliero; completo settimanale + differenziale giornaliero; completo settimanale + incrementale giornaliero).
ii. Applicazione delle stesse misure di sicurezza dei dati in ambiente di produzione.
iii. Custodia in luoghi sicuri con accesso limitato e controllato.
iv. Utilizzo di meccanismi di crittografia (attuali e non vulnerabili) in caso di impiego di dispositivi di storage esterni (ad es. su cloud, hard disk esterni, memorie esterne, siti di terzi, nastri magnetici, tra gli altri).
v. Obbligo di verifica periodica della corretta realizzazione delle copie di back-up e di ripristino.

XIII. Misure di sicurezza ambientali

Il Fornitore e i subappaltatori che realizzano il trattamento di dati personali per conto di BREBEMI, per la tutela delle risorse informatiche impiegate per la prestazione dei Servizi a BREBEMI devono adottare le misure di sicurezza ambientali elencate di seguito.

i. Misure di controllo dell'ambiente fisico in permutatori intermedi e principali (IDF, MDF), siti, ecc.
ii. Strumenti e procedure di monitoraggio di tali controlli (ad es. aria condizionata, gruppi di continuità UPS, rilevatori di umidità, allarmi antincendio, mezzi di estinzione incendio).
iii. I centri di dati devono disporre almeno dei seguenti controlli di sicurezza fisica:
    - Controllo accessi
    - Aria condizionata
    - Sistemi antincendio
    - Gruppo di continuità (UPS)
    - Telecamere a circuiti chiuso (CCTV).

XIV. Cancellazione ed eliminazione

Obblighi del Fornitore e dei subappaltatori che realizzano il trattamento di dati personali per conto di BREBEMI

i. Astenersi dal realizzare copie dei dati personali di BREBEMI, ad eccezione delle copie di back-up e di ripristino realizzate per motivi di sicurezza e comunque soggette ai requisiti di cui al presente documento.
ii. Astenersi dalla stampa di documenti contenenti dati personali di BREBEMI, salvo quando sia essenziale per la prestazione dei Servizi o la normale esecuzione del contratto. Distruggere i documenti che possono essere stampati una volta che non siano più necessari, in modo tale da impedire l'accesso intenzionale o accidentale di eventuali terzi alle informazioni, utilizzando, ad es. un distruggi documenti.
iii. Eliminare in modo sicuro le informazioni che risultino eccessive o irrilevanti per la prestazione dei servizi, con obbligo del Fornitore e dei suoi subappaltatori di assicurarsi che non possano essere recuperate con metodi semplici.
iv. Informare i propri dipendenti e collaboratori e impartire formazione sull'importanza di cancellare i dati personali dalle informazioni che non sono più necessarie, garantendone la riservatezza in ogni momento, in particolare al termine dell'incarico di trattamento dei dati.

XV. Dispositivi portatili o rimovibili

Obblighi del Fornitore e dei subappaltatori che realizzano il trattamento di dati personali per conto di BREBEMI su dispositivi portatili o rimovibili

i. Proteggere i dati personali di BREBEMI contenuti in tali dispositivi utilizzando meccanismi di crittografia attuali e non vulnerabili.
ii. Identificare i dispositivi portatili e/o rimovibili autorizzati e monitorare il loro uso.
iii. Condurre campagne di sensibilizzazione in materia di:

- rischi per la riservatezza e la protezione dei dati personali eventualmente derivanti dall'uso non autorizzato di dispositivi portatili e/o rimovibili;
- obbligo di segnalazione immediata di qualsiasi furto, perdita o danno di tali dispositivi.

XVI. Formazione e sensibilizzazione

Obblighi del Fornitore e dei subappaltatori che realizzano il trattamento di dati personali per conto di BREBEMI

i. Impartire formazione a dipendenti, personale esterno, amministratori, dirigenti e responsabili della sicurezza coinvolti nel trattamento delle informazioni riservate o dei dati personali di BREBEMI in materia di sicurezza informatica e di protezione dei dati personali in modo continuativo e regolare, adeguato ai loro ruoli e responsabilità.
ii. Implementare delle procedure per la valutazione del livello di conoscenza acquisito dopo queste azioni formative.
iii. Impartire formazione al personale coinvolto nel trattamento dei dati personali per conto di BREBEMI sulle misure di sicurezza di cui al presente documento.
iv. Tenersi aggiornati sulle nuove minacce e sulla loro evoluzione.

XVII. Controlli nel reclutamento e selezione di risorse umane

Obblighi del Fornitore e dei subappaltatori che realizzano il trattamento di dati personali per conto di BREBEMI

i. Includere nei loro processi di assunzione controlli volti a prevenire l'assunzione di dipendenti indagati, condannati o sanzionati per aver commesso crimini informatici o infrazioni degli obblighi di riservatezza legali o contrattuali, o garantire la loro stretta sorveglianza.
ii. Implementare misure specifiche in caso di estinzione del rapporto di lavoro dipendente, come comunicare in anticipo il licenziamento, il cambiamento o l'assenza per malattia dei dipendenti ai loro responsabili di sistema, oppure ricordare loro i rispettivi obblighi in materia di informazioni riservate e di protezione dei dati personali durante gli eventuali colloqui di uscita.

XVIII. MISURE DI RILEVAMENTO

Il Fornitore e i suoi subappaltatori devono stabilire dei controlli sulle risorse informatiche che permettono l'accesso ai dati personali di BREBEMI o in cui ne viene realizzato il trattamento, che consentano di verificare il corretto funzionamento e l'efficacia delle misure di sicurezza e l'identificazione tempestiva di qualsiasi evento o anomalia suscettibile di compromettere la riservatezza, l'integrità o la disponibilità di tali dati, essendo quindi obbligati a:

i. Tenere un registro storico degli eventi rilevati e del monitoraggio, per migliorare i processi e le misure di sicurezza.
ii. Analizzare gli eventi e le anomalie rilevate per determinare il loro obiettivo, la portata e i metodi di attacco, e se devono essere classificati o meno come incidenti di sicurezza.
iii. Condurre una valutazione d'impatto o degli effetti negativi che gli eventi o le anomalie di sicurezza rilevati potrebbero causare (Basso, Medio, Alto), assegnando in conformità a tale valutazione la rispettiva priorità alle azioni correttive.

XIX. Monitoraggio continuo

Il Fornitore e i suoi subappaltatori devono implementare le seguenti procedure e controlli per monitorare le risorse informatiche in cui si realizza il trattamento dei dati personali di BREBEMI o che ne permettono l'accesso.

i. **Monitoraggio preventivo e reattivo della rete**: mediante la generazione di avvisi in caso di rilevamento di eventi o anomalie, analisi degli stessi, generazione di documentazione delle prove sul monitoraggio con indicazione di data, ora e risultato, ecc.
ii. **Monitoraggio dell'attività del personale:** registrazione degli eventi rilevanti, definizione della periodicità del monitoraggio e del processo di verifica, frequenza della revisione dei file di log e portata: log di autenticazione (accessi falliti), log di cambi di configurazione, log di creazione, modifica e cancellazione di utenti, profili e privilegi, modifiche non autorizzate fatte da utenti validi; nonché reportistica finalizzata ai processi decisionali.
iii. **Rilevamento di codici malevoli.**
iv. **Monitoraggio dell'attività dei fornitori di servizi esterni:** ad es. accessi fisici non autorizzati al centro di elaborazione dati; accessi logici non autorizzati alle risorse di calcolo; blocco o apertura non autorizzata di porte; installazione non autorizzata di software; non conformità relative allo sviluppo di software sicuro.

XX. File di log

Il Fornitore e i subappaltatori che realizzano il trattamento di dati personali per conto di BREBEMI devono abilitare dei registri di audit nelle rispettive risorse informatiche impiegate a supporto della prestazione dei Servizi a BREBEMI, e come minimo i seguenti registri:

- Log di autenticazione (accessi falliti e riusciti)
- Log di cambiamenti di configurazione
- Log di creazione, modifica e cancellazione di utenti, profili e privilegi

Requisiti dei file di log

i. I file di log devono essere protetti da accessi non autorizzati e possibili alterazioni, e la configurazione e la revisione delle informazioni in essi contenute devono rispettare i requisiti di confidenzialità e di protezione dei dati personali;
ii. I file di log devono disporre di copie di backup e di ripristino;

iii. I file di log devono essere soggetti a revisione periodica per verificarne la corretta configurazione e funzionamento;
iv. I file di log di risorse informatiche che permettono l'accesso ai dati personali di BREBEMI o in cui ne viene realizzato il trattamento devono essere conservati sino al decorso dei termini di prescrizione delle sanzioni amministrative per violazione dei dati personali, ossia per un periodo minimo tre (3) anni, al fine di poter di svolgere accertamenti su eventuali violazioni dei dati personali da notificare alle autorità o agli interessati.

XXI. MISURE CORRETTIVE E NOTIFICHE

XXII. Piani di risposta e ripristino in caso di incidenti di sicurezza

Obblighi del Fornitore e dei suoi subappaltatori che accedono a informazioni confidenziali e dati personali di BREBEMI o che ne realizzano il trattamento per conto di quest'ultima

i. Disporre di piani di risposta e di ripristino in caso di incidenti di sicurezza suscettibili di compromettere la riservatezza, l'integrità e/o la disponibilità dei dati personali, in cui si prestabiliscano i tempi di risposta per ripristinare la normalità del trattamento dei dati personali effettuato per conto di BREBEMI in base alla loro criticità (misurata in termini di impatto e urgenza);
ii. Registrare e documentare gli incidenti di sicurezza che riguardano le risorse informatiche che permettono l'accesso ai dati personali di BREBEMI o in cui ne viene realizzato il trattamento, riportando almeno:
    - Data di rilevamento dell'incidente di sicurezza
    - Data di risoluzione o contenimento dell'incidente di sicurezza
    - Data di segnalazione dell'incidente di sicurezza
    - Breve descrizione dell'incidente di sicurezza
    - Numero di interessati (riferito solo a dati personali di BREBEMI)
    - Numero di registrazioni interessate (riferito solo a dati personali di BREBEMI)
    - Natura dell'incidente: intenzionale o accidentale
    - Se compromette la riservatezza, l'integrità o la disponibilità dei dati personali
    - Urgenza
    - Impatto
    - Risorse informatiche interessate
    - Misure preventive implementate prima dell'incidente di sicurezza
    - Misure correttive adottate per mitigare gli effetti negativi dell'incidente di sicurezza e prevenirne la reiterazione
    - Altre informazioni eventualmente richieste da BREBEMI
iii. Riferire immediatamente a BREBEMI qualsiasi incidente di sicurezza suscettibile di compromettere la riservatezza, l'integrità o la disponibilità dei dati personali trattati per conto suo, rivolgendosi all'indirizzo email **privacy@brebemi.it**, accludendo tutte le informazioni specificate al punto precedente.
iv. Testare periodicamente i piani di emergenza e di ripristino, documentando i risultati in modo appropriato.
v. Mantenere una comunicazione coordinata con i team di risposta agli incidenti di sicurezza (Computer Emergency Response Team, CERT) locali e altro

personale di sicurezza informatica, in base ai tipi di incidenti e alle rispettive risposte.

vi. Definire dei controlli attivabili in caso di rilevamento di incidenti di sicurezza per il contenimento e la risoluzione, come, tra gli altri, blocco di sessione, fine della sessione, blocco di connessioni remote, blocco di utenti in caso di ripetuti tentativi di accesso falliti, recupero dati attraverso l'uso di copie di backup, eccetera.

XXIII. Gestione delle vulnerabilità

Il Fornitore e i suoi subappaltatori devono porre rimedio alle vulnerabilità che, a seguito di regolari controlli o di eventi o incidenti di sicurezza, possono essere rilevate nelle risorse informatiche che permettono l'accesso ai dati personali di BREBEMI o in cui ne viene realizzato il trattamento, dovendo inoltre:

i. Disporre di procedure documentate disciplinanti la gestione di tali vulnerabilità, la riparazione delle stesse e l'aggiornamento dei controlli, e che devono identificare:
   - Le risorse informatiche
   - L'elenco delle minacce (tipologie e scenari di rischi, nonché categorizzazione per ciascuno di esse)
   - L'analisi dei rischi
   - Il trattamento e monitoraggio dei rischi rilevati.

ii. Condurre periodicamente scansioni di vulnerabilità (esterne e interne) e analizzare le vulnerabilità rilevate per il miglioramento continuo delle misure di sicurezza e dei controlli preventivi e di accertamento.

iii. Tenersi aggiornati con le notifiche di vulnerabilità dai CERT locali, da forum, notizie, siti web specializzati e altro personale di sicurezza informatica.

ALLEGATO IV. RICHIESTA DI AUTORIZZAZIONE DI NUOVI SUB-RESPONSABILI

AUTORIZZAZIONE DEI SUB-RESPONSABILI DEL TRATTAMENTO DI DATI

Titolare del trattamento:	Fare clic o premere qui per inserire il testo.
Responsabile del trattamento:	Fare clic o premere qui per inserire il testo.

I. Il Titolare del trattamento autorizza il Responsabile del trattamento a subappaltare alla ditta o ditte specificate di seguito i servizi altrettanto identificati di seguito:

a. Denominazione sociale	Fare clic o premere qui per inserire il testo.		
b. C.F./P.IVA:	Fare clic o premere qui per inserire il testo.		
c. Sede legale	Fare clic o premere qui per inserire il testo.		
d. Dati di contatto del Responsabile della protezione dei dati o della persona preposta alla protezione dei dati personali	Fare clic o premere qui per inserire il testo.		
e. Ubicazione da cui vengono prestati i servizi (località, paese)	Fare clic o premere qui per inserire il testo.		
f. Attività da realizzare per conto del Fornitore che implicano o richiedono il trattamento dei dati personali del Cliente:	Fare clic o premere qui per inserire il testo. ☐ Ricompilazione ☐ Strutturazione ☐ Ripristino ☐ Rivelazione ☐ Allineamento o combinazione ☐ Distruzione	☐ Registrazione ☐ Hosting/ Stoccaggio ☐ Consultazione o lettura ☐ Divulgazione ☐ Limitazione ☐ Altri …. Fare clic o premere qui per inserire il testo.....	☐Organizzazione ☐ Adattamento o alterazione ☐ Uso ☐ Messa a disposizione ☐ Cancellazione
g. Categoria di interessati	☐Candidati/ aspiranti a posto di lavoro ☐ Dipendenti ☐ Ex dipendenti ☐ Stagisti e personale iterino	☐ Fornitori (persone fisiche) ☐ Amministratori e Dirigenti ☐ Clienti ☐ Utenti di social network	☐ Visitatori dei locali di Brebemi ☐ Persone fisiche vulnerabili (minori, anziani o invalidi) ☐ Altri (specificare)…. Fare clic o premere qui per inserire il testo.....

h. Tipologie di dati	☐ Dati generici ☐ Credenziali di accesso o di identificazione ☐ Dati di contatto ☐ Carta d'identità, permesso di soggiorno o passaporto ☐ Affiliazione sindacale ☐ Sconosciuti	☐ Dati economico-finanziari ☐ Dati di localizzazione ☐ Dati su condanne penali e reati ☐ Convinzioni religiose o filosofiche ☐ Stato di salute	☐ Dati genetici ☐ Opinioni politiche ☐ Vita sessuale ☐ Dati biometrici (immagine facciale dati dattiloscopici) ☐ Altri (specificare)…. Fare clic o premere qui per inserire il testo…..

II. Il Responsabile del trattamento acconsente e si impegna, a titolo esemplificativo e non esaustivo, ad adempiere ai seguenti obblighi:

(i) Stipulare un Accordo sul trattamento dei dati con i sub-responsabili autorizzati vincolandoli contrattualmente ad adempiere almeno agli stessi obblighi del Fornitore nei confronti del Titolare del trattamento.

(ii) Fornire ai sub-responsabili autorizzati le istruzioni del caso impartite dal Titolare del trattamento per eseguire la prestazione dei servizi, vincolando contrattualmente il subappaltatore alla realizzazione del trattamento dei dati personali in conformità a tali istruzioni.

(iii) Vincolare contrattualmente i sub-responsabili autorizzati a limitare l'accesso e il trattamento dei dati personali alla prestazione dei servizi appaltati, con divieto di trasferimento o di divulgazione a terzi di tali dati.

(iv) Vincolare contrattualmente i sub-responsabili autorizzati all'attuazione delle misure di sicurezza tecniche e organizzative previste dal Contratto.

(v) Vincolare contrattualmente i sub-responsabili autorizzati a procedere, una volta conclusa la prestazione dei servizi che legittima il trattamento dei dati personali, e in conformità alle indicazioni del Titolare del trattamento, alla distruzione o alla restituzione di tutti i dati personali a cui hanno avuto accesso come conseguenza della prestazione dei servizi.

A [fare clic o premere qui per inserire il testo], addì [*] [fare clic o premere qui per inserire il testo] 20**

Per il Titolare del trattamento	**Per il Responsabile del trattamento**
[Nome] [Carica]	[Nome] [Carica]
[Nome] [Carica]	[Nome] [Carica]