Accordo per il Trattamento dei Dati

Diennea S.r.l. con sede legale in Viale G. Marconi 30/14, 48017, Faenza (RA), P. IVA 02243600398 ("**Diennea**", di seguito anche "**Fornitore**" o "**Responsabile**") e la controparte che accetta l'accordo che segue ("**Cliente**") hanno stipulato un contratto per la fornitura dei Servizi del Responsabile, o comunque un altro atto giuridico volto a disciplinare i rapporti tra le Parti, o, ancora, hanno posto in essere un comportamento concludente volto alla conclusione di un contratto che implica attività di trattamento di Dati Personali (di seguito, come di volta in volta modificato o aggiornato, solo il "**Contratto**").

Il presente accordo per il trattamento dei dati (compresi i suoi allegati, "**Accordo per il Trattamento dei Dati**") contiene le previsioni dell'art. 28 GDPR come interpretate dal Comitato Europeo per la protezione dei dati personali nell'Opinione 14/2019.

Il presente Accordo per il Trattamento Dati e in particolare la descrizione dei Servizi oggetto di Trattamento fatta nell'Allegato 1 prevale su qualsiasi accordo scritto o orale fatto prima della firma o dell'esecuzione del presente Accordo per il Trattamento dei Dati.

L'Accordo per il Trattamento dei Dati è concluso tra Diennea e il Cliente ed integra il Contratto. L'Accordo per il Trattamento dei Dati sarà efficace, e sostituirà qualsiasi altro accordo tra le Parti precedentemente applicabile in relazione allo stesso oggetto (comprese eventuali modifiche o addendum al trattamento dei dati relativi ai Servizi del Responsabile), a partire dalla Data di Entrata in Vigore e per tutta la Durata.

Il soggetto che sottoscrive il presente Accordo per il Trattamento dei Dati per conto del Cliente garantisce che: (a) ha il potere di rappresentanza per vincolare il Cliente al presente Accordo per il Trattamento dei Dati; e (b) sottoscrive, per conto del Cliente, il presente Accordo per il Trattamento dei Dati. Se non dispone del potere di rappresentanza per vincolare il Cliente, la preghiamo di non sottoscrivere il presente Accordo per il Trattamento dei Dati e di trasmetterlo al soggetto debitamente autorizzato a tali attività e in possesso del potere di firma e rappresentanza del Cliente.

1. Preambolo

1.1 L'Accordo per il Trattamento dei Dati riflette le intese intercorse tra le Parti rispetto al trattamento dei Dati Personali del Cliente come disciplinato dalla Legislazione europea e nazionale.

2. Definizioni

2.1 Tutti i termini con lettera maiuscola inseriti nell'Accordo per il Trattamento dei Dati hanno il seguente significato:

"**Autorità di Controllo**": si intende una "autorità di controllo" come definita nel GDPR.

"Clausole Contrattuali Standard": indica le Clausole Contrattuali Standard per i trasferimenti di dati personali verso paesi terzi secondo l'articolo 28(7) del Regolamento (EU) 2016/679 approvate dal Parlamento Europeo e dal Consiglio disponibili qui: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32021D0914&qid=1693412724244

"**Consociata**": indica un'entità giuridica, anche appartenente ad un gruppo societario, che direttamente o indirettamente ha il controllo ovvero è controllata da una parte.

"**Data di Entrata in Vigore**": si intende la data in cui il Cliente ha sottoscritto il Contratto o le Parti hanno altrimenti concordato l'efficacia del Contratto o dell'Accordo per il Trattamento dei Dati.

"**Dati Personali del Cliente**": si intendono i Dati Personali che vengono Trattati da Diennea per conto del Cliente nella fornitura dei Servizi del Responsabile da parte di Diennea.

"**Documentazione di Sicurezza**": si intende qualsiasi certificazione di sicurezza o documentazione (es. misure organizzative e tecniche di sicurezza, piani di disaster recovery e business continuity, ecc.) che il Fornitore rende disponibile in relazione ai Servizi del Responsabile. Rientrano in questa definizione, le evidenze di cui alla Sezioni 7.4 (Certificazione di sicurezza), 8 (Valutazioni d'impatto e consultazione preventiva), 11.3.(a) e 12.2 (Contatti del Fornitore e registro dei trattamenti), 17 (Assicurazione).

"**Durata**": si intende il periodo che va dalla Data di Entrata in Vigore fino al termine della fornitura da parte del Fornitore dei Servizi del Responsabile ai sensi del Contratto.

"**GDPR**": si intende il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla tutela delle persone fisiche con riguardo al Trattamento dei dati personali, nonché alla libera circolazione di tali dati, e che abroga la Direttiva 95/46/CE.

"**Incidente**": si intende una violazione della sicurezza di Diennea che comporta la distruzione accidentale o illecita, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai Dati Personali del Cliente su sistemi gestiti o altrimenti controllati dal Fornitore.

"**Indirizzo E-mail di Notifica**": si intende in successione alternativa, l'indirizzo e-mail: a) del Data Protection Officer del Cliente (se nominato); b) indicato dal Cliente nel Contratto; c) utilizzato dal Cliente durante l'erogazione dei Servizi del Responsabile per ricevere alcune notifiche di Diennea relative al presente Accordo per il Trattamento dei Dati.

"**Istruzioni Aggiuntive**": si intendono le istruzioni aggiuntive di cui all'Allegato 4.

"**Legislazione europea e nazionale**": si intende il GDPR e la legislazione dello Stato Membro dell'UE applicabile al Trattamento dei Dati Personali del Cliente.

"**Meccanismi di Trasferimento**": si intende una decisione vincolante emessa dalla Commissione Europea che permette il Trasferimento di dati personali dallo SEE verso un paese terzo il cui l'ordinamento interno fornisca un adeguato livello di tutela in materia di protezione dei dati personali. In tale definizione si intendono ricomprese le Clausole Contrattuali di Trasferimento di volta in volta approvate dalla Commissione Europea per il Trasferimento di dati personali nonché le norme vincolanti di impresa (BCRs).

"**Misure di Sicurezza**": si intende quanto indicato nella Sezione 7.1.1. (Misure di Sicurezza sui sistemi del Fornitore).

"**Parti**": indica il Cliente e Diennea.

"**SEE**": si intende lo Spazio Economico Europeo.

"**Servizi del Responsabile**": si intendono i servizi oggetto del Contratto e descritti collettivamente nell'Allegato 1.

"**Subresponsabili**": si intendono i terzi autorizzati ai sensi del presente Accordo per il Trattamento dei Dati a trattare i Dati

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

Personali del Cliente al fine di fornire, in tutto o in parte, i Servizi del Responsabile e/o qualsiasi supporto tecnico correlato.

2.2 I termini "**Dati Personali**", "**Dati Particolari**", "**Interessato**", "**Responsabile**", "**Titolare**", "**Trattamento**" hanno il significato indicato nel GDPR.
2.3 I termini "**includere**" e "**incluso**" sono illustrativi e non sono l'unico esempio di un particolare concetto.
2.4 Qualsiasi riferimento a una legge, regolamento, statuto o altro atto legislativo è un riferimento a quest'ultimi, come di volta in volta modificati o riformulati.
2.5 Ogni riferimento a "**Clausola**" è un riferimento alle clausole delle Clausole Contrattuali Standard. Ogni riferimento a "**Sezione**" è un riferimento alle sezioni di questo Accordo per il Trattamento dei Dati.
2.6 Se il presente Accordo per il Trattamento di Dati fosse tradotto in un'altra lingua e vi fosse una discrepanza tra il testo in italiano e il testo tradotto, prevarrà il testo in italiano.

3. Durata

3.1 Il presente Accordo per il Trattamento di Dati ha effetti per tutta la Durata e fino alla cancellazione da parte del Fornitore di tutti i Dati Personali del Cliente.

4. Ambito di Applicazione

4.1 **Applicazione dei Servizi del Responsabile**. Il presente Accordo per il Trattamento di Dati si applica solo ai servizi per i quali le Parti ne hanno concordato l'applicazione.
4.2 **Applicazione delle Istruzioni Aggiuntive**. Le Istruzioni Aggiuntive integrano il presente Accordo per il Trattamento dei Dati e formano parte integrante e sostanziale del medesimo.

5. Trattamento dei Dati Personali

5.1 **Ruoli, responsabilità e istruzioni**
5.1.1 Le Parti riconoscono e concordano che: (a) l'Allegato 1 descrive l'oggetto e i dettagli del trattamento dei Dati Personali del Cliente; (b) Diennea agisce come Responsabile per i Dati Personali del Cliente ai sensi della Legislazione europea e nazionale; (c) il Cliente agisce come Titolare o Responsabile, a seconda dei casi, dei Dati personali del Cliente ai sensi della Legislazione europea e nazionale; e (d) ciascuna parte si conformerà agli obblighi ad essa applicabili ai sensi della Legislazione europea e nazionale rispetto al Trattamento dei Dati Personali del Cliente.
5.1.2 **Autorizzazione da parte del terzo Titolare**. Se il Cliente agisce come Responsabile, il Cliente garantisce al Fornitore che le istruzioni e le azioni del Cliente in relazione ai Dati Personali del Cliente, compresa la nomina di Diennea come ulteriore Responsabile, sono state autorizzate dal rispettivo Titolare.
5.2 **Istruzioni del Cliente**. Con il presente Accordo per il Trattamento di Dati, il Cliente incarica Diennea di Trattare i Dati Personali del Cliente: (a) solo in conformità alla legge applicabile; (b) per fornire i Servizi del Responsabile e qualsiasi supporto tecnico correlato, ferma restando la facoltà del Responsabile di trattarli in forma anonimizzata e/o aggregata per finalità statistiche e di miglioramento dei Servizi del Responsabile; (c) come ulteriormente specificato/indicato dal Cliente attraverso l'uso da parte sua dei Servizi del Responsabile (incluse modifiche alle impostazioni e/o alle funzionalità dei Servizi del Responsabile) e di qualsiasi supporto tecnico correlato; (d) come documentato nel Contratto, incluso il presente Accordo per il Trattamento di Dati; ed (e) come ulteriormente documentato in qualsiasi comunicazione scritta fornita dal Cliente al Fornitore da intendersi come ulteriore istruzione ai fini del presente Accordo per il Trattamento di Dati.
5.3 **Conformità del Fornitore alle istruzioni**. Il Fornitore si atterrà alle istruzioni di cui alla Sezione 5.2 (Istruzioni del Cliente) a meno che la Legislazione europea o nazionale cui è soggetto il Fornitore non richieda a quest'ultimo di intraprendere un diverso o ulteriore Trattamento dei Dati Personali del Cliente (es. Trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale), nel qual caso il Fornitore informerà tempestivamente il Cliente all'Indirizzo E-mail di Notifica (a meno che tale legislazione non vieti al Fornitore di farlo per importanti motivi di interesse pubblico). In nessun caso il Responsabile sarà onerato dell'obbligo di procedere ad un esame giuridico esaustivo delle istruzioni scritte impartite dal Cliente.

6. Cancellazione ed esportazione dei dati

6.1 **Cancellazione ed esportazione per il periodo di Durata**
6.1.1 **Servizi del Responsabile con funzionalità di esportazione**. Se i Servizi del Responsabile includono la possibilità per il Cliente di esportare autonomamente e in formato interoperabile i Dati Personali del Cliente, il Fornitore assicura che tale operazione sia garantita per tutta la Durata, salvo diversi accordi scritti con il Cliente.
6.1.2 **Servizi del Responsabile con funzionalità di cancellazione**. Se i Servizi del Responsabile includono la possibilità per il Cliente di cancellare autonomamente i Dati Personali del Cliente, il Fornitore assicura che tale cancellazione dai propri sistemi sia realizzata non appena ragionevolmente possibile, a meno che la Legislazione europea e nazionale non richieda la conservazione.
6.1.3 **Servizi del Responsabile senza funzionalità di cancellazione e/o di estrazione**. Se nel corso della Durata i Servizi del Responsabile non includono la possibilità per il Cliente di estrarre e/o cancellare autonomamente i Dati Personali del Cliente, il Fornitore darà seguito ad ogni richiesta del Cliente per facilitare tale operazione nelle stesse modalità e tempi indicati rispettivamente nella Sezione 6.1.1 (Servizi del Responsabile con funzionalità di esportazione) e Sezione 6.1.2 (Servizi del Responsabile con funzionalità di cancellazione).
6.1.4 Il Responsabile potrà mantenere i Dati Personali del Cliente che siano stati conservati con regolari operazioni di backup nel rispetto dei protocolli di *disaster recovery* e *business continuity* del Responsabile e/o dei Subresponsabili, purché il Responsabile – fatto salvo quanto previsto dalla Sezione 5.2.b - non tratti, e non consenta ai propri Subresponsabili di trattare, in maniera attiva o intenzionale tali Dati Personali del Cliente per qualsivoglia finalità ulteriore rispetto alla fornitura dei Servizi del Responsabile.
6.2 **Cancellazione alla scadenza della Durata**. Fatto salvo quanto previsto nella Sezione 6.1.1 (Servizi del Responsabile con funzionalità di esportazione), alla scadenza della Durata, il Cliente ordina al Fornitore di cancellare tutti i Dati Personali del Cliente (incluse le copie esistenti) dai sistemi del Fornitore in conformità alla legge Legislazione europea e nazionale applicabile. Il Fornitore darà esecuzione a questa istruzione non appena ragionevolmente possibile, salvo che nei limiti in cui la Legislazione europea e nazionale non richieda la conservazione e salvo quanto previsto dalla Sezione 6.1.4.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

7. Sicurezza dei dati

7.1 **Misure di Sicurezza e assistenza da parte del Fornitore**

7.1.1 **Misure di Sicurezza sui sistemi del Fornitore**. Il Fornitore adotterà e manterrà misure tecniche e organizzative per proteggere i Dati Personali del Cliente da distruzione accidentale o illecita, perdita, alterazione, divulgazione o accesso non autorizzati come descritto nell'Allegato 2. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del Trattamento posti in essere con i Servizi del Responsabile, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, l'Allegato 2 deve comprendere, se del caso, misure di sicurezza atte a: (a) cifrare i dati personali; (b) contribuire a garantire la riservatezza, l'integrità, la disponibilità e la resilienza costanti dei sistemi e dei servizi del Fornitore; (c) contribuire a ripristinare tempestivamente i dati personali a seguito di un incidente; e (d) verificarne periodicamente l'efficacia. Il Fornitore ha il diritto di aggiornare o modificare di tanto in tanto le Misure di Sicurezza, a condizione che tali aggiornamenti e modifiche non comportino il deterioramento della sicurezza complessiva dei Servizi del Responsabile.

7.1.2 **Misure di Sicurezza per il personale del Fornitore**. Il Fornitore adotterà misure adeguate per garantire il rispetto delle Misure di Sicurezza da parte di tutti coloro che operano sotto la sua autorità compresi i propri dipendenti, agenti, appaltatori e Subresponsabili nella misura a loro applicabile secondo la prestazione effettivamente svolta, inclusa l'assicurazione sul fatto che tutte le persone autorizzate a trattare i Dati Personali del Cliente si sono impegnate alla riservatezza o sono soggette a un adeguato obbligo di riservatezza in conformità con la Legislazione europea e nazionale.

7.1.3 **Assistenza sulla sicurezza dei dati da parte del Fornitore**. Il Cliente accetta che Diennea (tenendo conto della natura del Trattamento dei Dati Personali del Cliente e delle informazioni a disposizione di Diennea) assisterà il Cliente nel garantire il rispetto di eventuali obblighi del Cliente in materia di sicurezza dei dati personali e violazioni dei dati personali, compresi (se del caso) gli obblighi del Cliente ai sensi degli articoli da 32 a 34 GDPR, attraverso:
a) l'attuazione e manutenzione delle Misure di Sicurezza conformemente alla Sezione 7.1.1. (Misure di Sicurezza sui sistemi del Fornitore);
(b) l'attuazione di quanto indicato nella Sezione 7.2 (Incidenti sui dati); e
(c) fornendo al Cliente la Documentazione di Sicurezza in conformità alla Sezione 7.5.1 (Revisione della Documentazione di Sicurezza) e le informazioni previste nel presente Accordo per il Trattamento dei Dati.

7.2 **Incidenti sui dati**

7.2.1 **Notifica di Incidente**. Se il Fornitore viene a conoscenza di un Incidente, il Fornitore: (a) informerà il Cliente dell'Incidente tempestivamente e senza indebiti ritardi; e (b) adotterà tempestivamente misure ragionevoli per ridurre al minimo le conseguenze e proteggere i Dati Personali del Cliente.

7.2.2 **Dettagli dell'Incidente**. Le notifiche effettuate ai sensi della Sezione 7.2.1 (Notifica di Incidente) descriveranno per quanto possibile i dettagli dell'Incidente, comprese le misure adottate per ridurre i potenziali rischi e le misure che Diennea raccomanda al Cliente di adottare per affrontare l'Incidente.

7.2.3 **Invio della notifica**. Il Fornitore invierà la notifica di qualsiasi Incidente all'Indirizzo E-mail di Notifica o, a discrezione di Diennea, tramite altre comunicazioni dirette (ad esempio, tramite telefonata o riunione de visu). Il Cliente è l'unico responsabile per garantire che l'Indirizzo E-mail di Notifica sia attuale, valido e monitorato.

7.2.4 **Notifica verso terzi**. Il Cliente è l'unico responsabile per l'osservanza delle obbligazioni relative alle notifiche di incidenti applicabili al Cliente e dell'adempimento di qualsiasi obbligo di notifica/comunicazione nei confronti di terzi in relazione a qualsiasi Incidente.

7.2.5 **Valore della notifica**. La notifica o la risposta di Diennea a un Incidente ai sensi della presente Sezione 7.2 (Incidenti sui dati) non sarà interpretata come un riconoscimento da parte di Diennea di alcuna colpa o responsabilità in relazione all'Incidente.

7.3 **Responsabilità e valutazione della sicurezza da parte del Cliente**

7.3.1 **Responsabilità del Cliente sulla sicurezza**. Fatti salvi gli obblighi del Fornitore ai sensi delle Sezioni 7.1 (Misure di Sicurezza e assistenza da parte del Fornitore) e 7.2 (Incidenti sui dati), il Cliente accetta che:
(a) è l'unico responsabile per l'utilizzo dei Servizi del Responsabile, e in particolare:
(i) dell'uso appropriato dei Servizi del Responsabile in modo da garantire un livello di sicurezza adeguato al rischio in relazione ai Dati Personali del Cliente; e
(ii) della protezione delle credenziali di autenticazione degli account, sistemi e dispositivi utilizzati dal Cliente per accedere ai Servizi del Responsabile; e
(b) Diennea non ha alcun obbligo di proteggere i Dati Personali del Cliente che il Cliente sceglie di memorizzare o trasferire al di fuori dei sistemi di Diennea e dei suoi Subresponsabili.

7.3.2 **Valutazione della sicurezza da parte del Cliente**. Il Cliente riconosce e concorda che (tenendo conto dello stato dell'arte, dei costi di implementazione e della natura, portata, contesto e finalità del Trattamento dei Dati Personali del Cliente, nonché dei rischi per le persone fisiche) le misure di sicurezza attuate e mantenute da Diennea come indicato nella Sezione 7.1.1 (Misure di Sicurezza sui Sistemi del Fornitore) forniscono un livello di sicurezza adeguato al rischio connesso al trattamento dei Dati Personali del Cliente.

7.4 **Certificazione di sicurezza**. Per valutare e contribuire a garantire la continua efficacia delle Misure di Sicurezza, il Fornitore potrebbe, a sua libera discrezione, integrare le Misure di Sicurezza e la Documentazione di Sicurezza con l'ottenimento di certificazioni (es. ISO27001), codici di condotta e/o meccanismi di certificazione.

7.5 **Verifiche e audit**

7.5.1 **Revisione della Documentazione di Sicurezza**. Per dimostrare il rispetto da parte del Fornitore degli obblighi previsti dal presente Accordo per il Trattamento dei Dati, il Fornitore metterà a disposizione del Cliente la Documentazione di Sicurezza.

7.5.2 **Diritto di audit da parte del Cliente.** Le Parti convengono che:
(a) il Fornitore consentirà al Cliente o a un terzo revisore designato dal Cliente di effettuare verifiche (incluse ispezioni) per verificare il rispetto da parte del Fornitore degli obblighi derivanti dal presente Accordo per il Trattamento dei Dati in conformità con la Sezione 7.5.3 (Condizioni aggiuntive per gli audit). Il Fornitore contribuirà a tali audit in conformità con la presente Sezione 7.5 (Verifiche e audit);
(b) il Cliente può anche condurre un audit per verificare la conformità del Fornitore agli obblighi previsti dal presente Accordo

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

per il Trattamento dei dati anche mediante l'esame della documentazione di cui alla Sezione 7.4 (che riflette l'esito di un audit condotto da un auditor terzo).

7.5.3 **Condizioni aggiuntive per gli audit.** Per lo svolgimento di audit:

(a) il Cliente invierà al Fornitore qualsiasi richiesta di verifica ai sensi della Sezione 7.5.2(a) all'indirizzo audit@diennea.com;

(b) in seguito al ricevimento da parte del Fornitore di una richiesta ai sensi della Sezione 7.5.3(a), il Cliente e il Fornitore discuteranno e concorderanno in anticipo l'identità dell'auditor, la data di inizio - che in ogni caso non potrà essere identificata prima che siano decorsi venti (20) giorni lavorativi dalla data in cui il Responsabile riceva la richiesta di audit da parte del Cliente - nonché la portata e la durata, i controlli su sicurezza e riservatezza in relazione ad ogni audit;

(c) il Cliente riconosce e accetta che i costi dallo stesso sostenuti per le attività di audit sono a proprio esclusivo carico; il Cliente ha facoltà di svolgere, senza alcun costo, un audit sul Fornitore della durata di un (1) giorno lavorativo entro l'anno solare di riferimento, fermo restando il diritto del Fornitore di addebitare costi e oneri al Cliente per ogni eventuale ed ulteriore attività di audit non prevista ai sensi del presente articolo;

(d) il Fornitore può opporsi a qualsiasi revisore terzo nominato dal Cliente per effettuare audit ai sensi della Sezione 7.5.2(a) se, a ragionevole parere di Diennea, non è adeguatamente qualificato o indipendente; è un concorrente di Diennea o altrimenti manifestamente inadatto all'attività. Qualsiasi obiezione di questo tipo da parte di Diennea richiederà al Cliente di nominare un altro revisore o di condurre direttamente l'audit stesso;

(e) Il Cliente è informato e accetta che le attività di audit dovranno tenere conto delle regole relative ai criteri di sicurezza e/o riservatezza che possono eventualmente imporre limiti all'estensione dell'audit. In particolare, nessuna disposizione del presente Accordo per il Trattamento dei Dati può richiedere al Fornitore di rivelare o consentire l'accesso al Cliente o al suo revisore terzo a:

(i) dati di qualsiasi altro cliente del Fornitore;
(ii) informazioni contabili o finanziarie interne al Fornitore;
(iii) segreti commerciali e know how del Fornitore;
(iv) qualsiasi informazione che, secondo la ragionevole opinione di Diennea, potrebbe compromettere la sicurezza dei sistemi o dei locali di Diennea; o far sì che Diennea violi gli obblighi derivanti dalla Legislazione europea sulla protezione dei dati o i suoi obblighi di sicurezza nei confronti del Cliente o di terzi; oppure
(v) qualsiasi informazione alla quale il Cliente o il suo terzo revisore cerchi di accedere per ragioni diverse dall'adempimento in buona fede degli obblighi del Cliente ai sensi della Legislazione europea e nazionale;

(f) lo svolgimento delle attività di verifica e controllo è condizionato alla conclusione di uno specifico accordo di riservatezza tra tutte le parti coinvolte.

8. Valutazioni d'impatto e consultazione preventiva

8.1 Previa richiesta del Cliente formulata con congruo anticipo, Diennea (tenendo conto della natura del Trattamento e delle informazioni a disposizione di Diennea) assisterà il Cliente nel garantire il rispetto di eventuali obblighi del Cliente in materia di valutazioni d'impatto sulla protezione dei dati e di consultazione preventiva, compresi (se del caso) gli obblighi del Cliente ai sensi degli articoli 35 e 36 GDPR, attraverso: (a) la fornitura della Documentazione di Sicurezza conformemente alla sezione 7.5.1 (Revisione della Documentazione di Sicurezza); (b) la fornitura di informazioni contenute nel presente Accordo per il Trattamento dei Dati; e (c) la fornitura o la messa a disposizione, in conformità con le prassi standard di Diennea, di altri materiali relativi ai Servizi del Responsabile e al Trattamento dei Dati Personali del Cliente (ad esempio, materiale di assistenza).

9. Diritti degli Interessati

9.1 **Risposte alle richieste degli Interessati**. Se il Fornitore riceve una richiesta da un Interessato in relazione ai Dati Personali del Cliente, il Fornitore consiglierà all'Interessato di presentare la sua richiesta all'Indirizzo E-mail di Notifica (o, ove opportuno e/o possibile, informerà direttamente il Cliente della richiesta inoltrando la stessa all'Indirizzo E-mail di Notifica), e il Cliente sarà responsabile di gestire tale richiesta.

9.2 **Assistenza del Fornitore per le richieste degli Interessati**. Il Cliente accetta che Diennea (tenendo conto della natura del trattamento dei Dati Personali del Cliente) assisterà il Cliente nell'adempimento di qualsiasi obbligo del Cliente rispetto alle richieste di esercizio dei diritti dell'Interessato di cui al Capitolo III GDPR attraverso: (a) ove possibile, la messa a disposizione di funzionalità specifiche nei Servizi del Responsabile; (b) il rispetto degli impegni di cui alla Sezione 9.1 (Risposte alle richieste degli Interessati). Il Cliente riconosce e accetta che, nel caso in cui tale cooperazione e assistenza richiedano un impiego significativo di risorse da parte del Responsabile e il Cliente sia in grado di acquisire in autonomia tali informazioni, tale sforzo sarà addebitabile, previo preavviso e accordo, al Cliente.

10. Trasferimenti di Dati Personali

10.1 **Strutture per la memorizzazione e l'elaborazione dei dati**. Il Cliente accetta e autorizza il Fornitore affinché possa trattare (anche tramite Subresponsabili) i Dati Personali del Cliente all'interno e all'esterno dello SEE purché tali Trattamenti siano sorretti da idonei Meccanismi di Trasferimento, da indicare nell'Allegato 3.

10.2. **Meccanismo di trasferimento dei subresponsabili**. Qualora il Fornitore intenda avvalersi di uno o più subresponsabili stabiliti al di fuori del SEE e non siano disponibili altri meccanismi di trasferimento diversi dalle Clausole Contrattuali Standard, le Parti convengono che: (a) il Fornitore e il suo o i suoi subresponsabili saranno considerati "parti" ai sensi del "MODULO TRE: Trasferimento da responsabile a responsabile" delle Clausole Contrattuali Standard; (b) gli Allegati 1--4 del presente DPA sostituiranno o saranno sostanzialmente riflessi negli allegati delle Clausole Contrattuali Standard.

11. Subresponsabili

11.1 **Autorizzazione all'impiego di Subresponsabili**. Il Cliente conferisce autorizzazione generale all'impiego di Subresponsabili per l'erogazione dei Servizi del Responsabile.

11.2 **Informazioni sui Subresponsabili**. L'elenco aggiornato e le rispettive informazioni sui Subresponsabili sono disponibili come meglio indicato nell'Allegato 3 al presente Accordo per il Trattamento dei Dati.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

11.3 **Requisiti per il coinvolgimento dei Subresponsabili**. Quando impiega un Subresponsabile, il Fornitore:
(a) garantirà tramite un contratto scritto o un altro atto giuridico vincolante che:
(i) il Subresponsabile acceda ed utilizzi i Dati Personali del Cliente solo nella misura necessaria per adempiere agli obblighi a lui affidati in subappalto, in conformità con il Contratto (incluso il presente Accordo per il Trattamento dei Dati) e – ove applicabile - con i Meccanismi di Trasferimento;
(ii) gli stessi obblighi di protezione dei dati di cui all'articolo 28(3) GDPR nonché le principali obbligazioni del presente Accordo per il Trattamento dei Dati siano imposti al Subresponsabile (o in ogni caso che le obbligazioni assunte offrano garanzie non inferiori a quelle offerte dal Responsabile);
(b) rimane pienamente responsabile di tutti gli obblighi subappaltati al Subresponsabile nonché di tutti gli atti e le omissioni di quest'ultimo.
11.4 **Possibilità di opporsi alle modifiche dei Subresponsabili.** Le Parti convengono che:
(a) per tutta la Durata, il Fornitore notificherà preventivamente al Cliente l'intenzione di impiegare nuovi Subresponsabili per il Trattamento dei Dati Personali del Cliente, utilizzando l'Indirizzo E-mail di Notifica, in modo tale che la mancata opposizione del Cliente – entro 10 giorni dalla notifica di cui alla presente Sezione - possa dimostrare (anche tacitamente) il consenso all'impiego di ogni Subresponsabile. Tale comunicazione includerà il nome, l'attività svolta, il Paese di stabilimento dei Subresponsabili impiegati;
(b) in caso di opposizione del Cliente a qualsiasi dei nuovi Subresponsabili, le Parti si impegnano a collaborare in buona fede per individuare soluzioni idonee a consentire la prosecuzione del Contratto e, ove ciò non sia possibile, è fatto salvo il diritto di ciascuna Parte di recedere dal Contratto e dall'Accordo per il Trattamento dei Dati dandone comunicazione scritta all'altra Parte entro 30 giorni dall'opposizione del Cliente all'impiego dei nuovi Subresponsabili come descritto nella Sezione 11.4(a).

12. Contatti del Fornitore e registro dei trattamenti

12.1 **Contatti del Fornitore**. Il Cliente può contattare Diennea in relazione a tutto quanto contenuto nel presente Accordo per il Trattamento dei Dati al seguente indirizzo: dpo@diennea.com.
12.2 **Registro dei trattamenti**. Il Cliente riconosce che Diennea è tenuto ai sensi del GDPR a: (a) raccogliere e conservare certe informazioni, compresi il nome e i dati di contatto di ciascun Responsabile e Titolare per conto del quale Diennea agisce e (se nominati) del rappresentante e del Responsabile della protezione dei dati; e (b) mettere tali informazioni a disposizione di qualsiasi Autorità di Controllo. Di conseguenza, il Cliente fornirà tali informazioni a Diennea attraverso i contatti indicati nella Sezione 12.1 o attraverso qualsiasi altro mezzo fornito da Diennea, impegnandosi a garantire che tutte le informazioni fornite siano sempre accurate e aggiornate.

13. Conflitti

13.1 **Conflitti tra gli accordi delle Parti.** In caso di conflitto o incoerenza tra le previsioni del Contratto, dell'Accordo per il Trattamento dei Dati e le Istruzioni Aggiuntive, si applica il seguente ordine di prevalenza: (a) le Istruzioni Aggiuntive; (b) le restanti previsioni dell'Accordo per il Trattamento dei Dati; e (c) le restanti previsioni del Contratto. Fatte salve eventuali modifiche dell'Accordo per il Trattamento dei Dati, il Contratto rimane pienamente valido ed efficace.
13.2 **Violazioni di norme di legge o di regolamento**. Ogni previsione del Contratto, dell'Accordo per il Trattamento dei Dati e/o delle Istruzioni Aggiuntive contraria alla Legislazione europea e nazionale deve intendersi come non riportata e integralmente sostituita dalla norma violata nel caso in cui non sia derogabile da un accordo tra le Parti.

14. Modifiche

14.1 **Modifiche agli Allegati**. Periodicamente, il Fornitore può modificare il contenuto degli Allegati, se è espressamente consentito dall'Accordo per il Trattamento dei Dati. Il Fornitore può modificare l'elenco dei Servizi del Responsabile inseriti nell'Allegato 1 solo: (a) per riflettere una modifica della denominazione di un servizio; (b) per aggiungere un nuovo servizio; oppure (c) sopprimere un servizio in uno dei due casi: (i) tutti i contratti per la fornitura di tale servizio sono terminati; o (ii) il Fornitore ha ricevuto il consenso del Cliente.
14.2 **Modifiche all'Accordo per il Trattamento dei Dati**. Diennea può modificare il presente Accordo per il Trattamento dei Dati se la modifica:
(a) è espressamente consentita dall'Accordo per il Trattamento dei Dati;
(b) è obbligatoria per rispettare la legge applicabile, una sentenza o altro provvedimento di un tribunale o gli orientamenti emanati da un'Autorità di Controllo o un'autorità governativa;
(c) non comporta un peggioramento della sicurezza complessiva dei Servizi del Responsabile;
(d) non amplia l'ambito di applicazione del (o elimina eventuali restrizioni al) diritto di Diennea di trattare i dati nell'ambito delle Istruzioni Aggiuntive o il suo trattamento dei Dati Personali del Cliente come indicato nella Sezione 5.3 (Conformità di Diennea alle istruzioni);
(e) non ha altrimenti un impatto negativo sui diritti del Cliente ai sensi del presente Accordo per il Trattamento dei Dati, come ragionevolmente determinato da Diennea.
14.3 **Notifica delle modifiche**. Ad eccezione dell'ipotesi indicata alla Sezione 14.2(b) ove la modifica è immediatamente in vigore tra le parti, se Diennea intende modificare il presente Accordo per il Trattamento dei Dati ai sensi della Sezione 14.2, Diennea informerà il Cliente almeno 30 giorni (o un periodo più breve eventualmente richiesto per conformarsi alla legge applicabile) prima che la modifica entri in vigore, inviando un'e-mail all'Indirizzo E-mail di Notifica. In caso di opposizione del Cliente a tali modifiche, le Parti si impegnano a collaborare in buona fede per individuare soluzioni idonee a consentire la prosecuzione del Contratto e, ove ciò non sia possibile, ciascuna Parte può recedere dal Contratto dandone comunicazione scritta all'altra Parte entro 30 giorni dalla comunicazione della modifica da parte di Diennea; in mancanza di esercizio della facoltà di recesso entro il suddetto termine, la modifica è vincolante tra le Parti a tutti gli effetti di legge e di contratto.

15. Responsabilità e risarcimento

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

15.1 **Perimetro del risarcimento del danno**. Le Parti riconoscono e accettano che qualora l'Interessato ("**Danneggiato**") lamenti, contro le Parti, di aver subito un danno – materiale o immateriale – causato da una violazione della Legislazione europea e nazionale:
(a) la Parte a cui risulti direttamente imputabile la responsabilità della violazione, ai sensi dell'art. 82(2) GDPR, risponderà interamente per il danno materiale o immateriale cagionato all'Interessato dichiarando sin d'ora di manlevare e tenere indenne l'altra Parte, qualora non abbia adempiuto agli obblighi della Legislazione europea e nazionale ad essa specificamente diretti;
(b) qualora il Fornitore e il Cliente siano coinvolti nello stesso Trattamento e siano entrambi responsabili del danno causato al Danneggiato, ai sensi dei commi 2 e 3 dell'art. 82 GDPR, ciascuno dei due sarà responsabile in solido per l'intero ammontare del danno, fermo, per entrambi, il diritto di rivalsa sull'altro per la quota di risarcimento allo stesso spettante in base al danno causato, come definito alla Sezione 16.2 (Negoziazione);
(c) nel caso in cui il danno causato al Danneggiato sia dovuto alla violazione delle disposizioni del presente Accordo per il Trattamento di Dati o della Legislazione europea e nazionale e sia imputabile interamente al Fornitore, il Fornitore è tenuto a risarcire interamente il Cliente, qualora quest'ultimo abbia provveduto, in tutto o in parte, al risarcimento del danno al Danneggiato;
(d) ciascuna Parte dovrà indennizzare o risarcire l'altra Parte qualora e nella misura in cui abbia contribuito a causare il danno lamentato dal Danneggiato o non abbia adottato appropriate misure di mitigazione, o abbia violato disposizioni del presente Accordo per il Trattamento di Dati o della Legislazione europea e nazionale.
15.2 **Negoziazione**. Nel caso indicato alla Sezione 15.1(c), la misura dell'indennizzo o del risarcimento, parametrata alla porzione di responsabilità in merito all'entità del danno cagionato è stabilita congiuntamente dalle Parti mediante accordo negoziato in buona fede.
15.3 **Foro competente**. In caso di controversie relative all'esecuzione o interpretazione del presente Accordo per il Trattamento di Dati, le Parti assegnano la competenza esclusiva al foro già individuato nel Contratto, con espressa deroga a quanto eventualmente diversamente stabilito da leggi o convenzioni internazionali.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

Allegato 1

A. Elenco delle Parti

Titolare: indica il Cliente come definite nel Contratto.

Responsabile:

1. **Nome:** Diennea S.r.l.
   Via: Viale G. Marconi n. 30/14 – 48018 Faenza (RA)
   DPO: ICTLC S.P.A.
   Contatto del DPO: dpo@diennea.com

B. Descrizione dei Trattamenti

Natura e finalità del Trattamento e dei Servizi del Responsabile

Il Fornitore tratterà Dati Personali del Cliente al fine di fornire i Servizi del Responsabile, come definiti nel Contratto sottoscritto tra il Cliente e il Fornitore, in conformità con le istruzioni contenute nell'Accordo per il Trattamento dei Dati.
A seconda dei Servizi del Responsabile scelti nel Contratto, i Dati Personali del Cliente potrebbero includere i seguenti Dati Personali:

Tipi di Interessati coinvolti	• Candidati • Clienti • Prospect • Consulenti/Collaboratori Esterni • Contraenti • Dipendenti • Dirigenti • Dipendenti di società appaltatrici • Familiari • Fornitori • Lavoratori somministrati • Legali • Minori • Partecipanti agli eventi • Tirocinanti/Stagisti • Visitatori • Soggetti i cui Dati Personali sono Trattati dal Cliente nell'ambito di fruizione dei Servizi del Responsabile
Dati personali Trattati	• Dati raccolti da tecnologie traccianti e dispositivi • Dati identificativi comuni (es. nome, cognome, indirizzo email) • Codice fiscale • Dati su abitudini di vita, consumi e comportamento • Dati su familiari/stato familiari • Immagine, video, suoni • Ulteriori categorie di Dati Personali Trattati dal Cliente tramite i Servizi del Responsabile

Frequenza del Trattamento

Per tutto l'arco temporale di esecuzione del Contratto.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

Durata del Trattamento

Il Trattamento avrà la medesima durata del Contratto per come definito nell'Accordo per il Trattamento dei Dati e fino alla cancellazione da parte del Fornitore di tutti i Dati Personali del Cliente.

Per il Trattamento da parte di subresponsabili, specificare anche l'oggetto, la natura e la durata del Trattamento

Si prega di fare riferimento all'Allegato 3 per ulteriori informazioni in merito.

C. Autorità di controllo competente

Autorità Garante per la protezione dei dati personali (Italia).

Le Parti potrebbero aggiornare di volta in volta la lista dei tipi di Dati Personali Trattati nell'erogazione dei Servizi del Responsabile.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

Allegato 2: Misure di sicurezza

Descrizione delle misure di sicurezza tecniche ed organizzative
Il Responsabile ed i Subresponsabili si impegnano a garantire un livello di sicurezza non inferiore a quello previsto dalle misure tecniche e organizzative di seguito descritte.

Informazioni sulle misure di sicurezza

Gestione della sicurezza delle informazioni
La Direzione dovrebbe definire una serie di politiche e misure per chiarire gli obiettivi al fine di supportare la sicurezza delle informazioni. A livello apicale, dovrebbe essere prevista una "Policy per la sicurezza delle informazioni" di carattere generale.

Organizzazione della sicurezza delle informazioni

Organizzazione interna
I ruoli e le responsabilità per la sicurezza delle informazioni sono definiti e assegnarti singolarmente a soggetti determinati. I compiti sono separati per ruoli e persone al fine di evitare conflitti di interesse e prevenire attività inappropriate.

Dispositivi mobili e telelavoro
È prevista una Policy di sicurezza e adeguati controlli per i dispositivi mobili (come laptop, tablet, PC, dispositivi indossabili, smartphone, strumenti USB e altri) e per il telelavoro.
La cifratura del disco è disponibile su tutti i dispositivi.

Sicurezza delle risorse umane

Prima dell'instaurazione del rapporto di lavoro
Le responsabilità in materia di sicurezza delle informazioni sono prese in considerazione durante l'assunzione di dipendenti, collaboratori e personale temporaneo (ad esempio attraverso adeguate descrizioni sulle mansioni da svolgere, controlli preassunzione) e inserite all'interno dei contratti (ad esempio con termini e condizioni del rapporto di lavoro e sottoscrizione di ulteriori accordi volti a definire ruoli e responsabilità in tema di sicurezza, obblighi di conformità, ecc.).

Durante il rapporto di lavoro
I manager si assicurano che i dipendenti e i collaboratori siano consapevoli e motivati a rispettare i loro obblighi per garantire la sicurezza delle informazioni. È stato formalizzato un procedimento disciplinare per gestire anche gli incidenti relativi alla sicurezza delle informazioni presumibilmente causati dai lavoratori, come previsto dal CCNL applicabile.

Conclusione o modifiche al rapporto di lavoro
Gli aspetti relativi alla sicurezza al momento dell'uscita di una persona dall'organizzazione, o nelle ipotesi di modifiche significative al ruolo ricoperto, sono gestiti attraverso procedure per la restituzione delle informazioni e delle apparecchiature aziendali in possesso del soggetto uscente, aggiornando i loro permessi di accesso, nonché ricordando loro la persistenza degli obblighi in materia di protezione dei dati, proprietà intellettuale, condizioni contrattuali, leggi ecc. ed anche ai doveri etici.

Gestione delle risorse del patrimonio aziendale

Responsabilità delle risorse del patrimonio aziendale
Tutte le informazioni relative alle risorse del patrimonio aziendale sono inventariate ed i relativi soggetti di riferimento identificati al fine di individuare le responsabilità per la loro sicurezza. È prevista una Policy per un "uso corretto" delle stesse e le risorse vengono restituite all'organizzazione al momento dell'uscita dei soggetti coinvolti.

Classificazione delle informazioni
Le informazioni sono classificate e catalogate dai rispettivi soggetti di riferimento in linea con quanto previsto dalle esigenze di sicurezza, nonché gestite in modo appropriato.

Gestione dei media
Le informazioni conservate sui media sono gestite, controllate, modificate ed utilizzate in modo tale da non comprometterne il loro contenuto. Tutti i documenti e i dati vengono mostrati solo a coloro che dispongono di profili di autorizzazione adeguati.

Controllo degli accessi

Requisiti aziendali per il controllo degli accessi
I requisiti dell'organizzazione per controllare l'accesso alle informazioni relative al patrimonio aziendale sono chiaramente documentati in una Policy per il controllo degli accessi e delle relative procedure. L'accesso alla rete e le connessioni prevedono limitazioni.

Gestione dell'accesso degli utenti
L'allocazione dei diritti d'accesso agli utenti è controllata dalla registrazione iniziale dell'utente fino alla rimozione del profilo quando esso non sia più necessario, incluse speciali restrizioni per i diritti di accesso privilegiato e la regolare gestione delle password. I diritti di accesso sono regolarmente revisionati e aggiornati.

Responsabilità degli utenti
Gli utenti sono consapevoli delle proprie responsabilità attraverso il mantenimento di un effettivo controllo degli accessi, ad es. scegliendo password complesse e mantenendole riservate.

Sistemi e applicazioni per il controllo degli accessi
L'accesso alle informazioni è limitato coerentemente a quanto previsto dalla Policy sul controllo degli accessi, ad es. attraverso autenticazioni sicure, gestione delle password, controllo delle utilità privilegiate e limitazioni all'accesso ai codici sorgente dei programmi.

Crittografia

Controllo crittografico
È prevista una Policy sull'uso della cifratura dei dati, oltre ad autenticazioni criptate e controlli di integrità, come firme digitali e

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

messaggi con codici di autenticazione, nonché una gestione delle chiavi di cifratura.

Sicurezza fisica e ambientale

Aree sicure
L'organizzazione ha definito un perimetro fisico e una recinzione, con controllo fisico degli accessi e procedure operative, in grado di proteggere i locali, gli uffici, le stanze, le aree di carico/scarico da accessi non autorizzati. Si prevede altresì la consulenza di uno specialista per quanto riguarda le misure di protezione contro incendi, allagamenti, terremoti, esplosioni, ecc.

Apparecchiatura
L'apparecchiatura (intesa perlopiù come apparecchiatura in ambito ICT), i servizi di supporto e il cablaggio sono essere resi sicuri e manutenuti. L'apparecchiatura e le informazioni non devono uscire dal loro luogo di riferimento se non previa autorizzazione, e in ogni caso sono adeguatamente protette sia all'interno che all'esterno del loro luogo di riferimento. Le informazioni vengono distrutte prima di procedere allo smaltimento o al riciclo dei dispositivi sui cui erano conservate. Le apparecchiature non protette sono rese sicure ed è previsto un apposito spazio ed una Policy di verifica.

Sicurezza delle operazioni

Procedure e responsabilità operative
Le procedure e le responsabilità operanti per l'area IT sono documentate. I cambiamenti alle infrastrutture ed ai sistemi IT sono controllati. Sono gestiti i singoli poteri e le relative prestazioni. I sistemi di sviluppo, quelli di verifica e quelli operativi sono separati.

Protezione da malware
Tutti i dispositivi sono protetti contro malware e gli utenti vengono sensibilizzati sul punto al fine di maturare un'idonea consapevolezza.

Backup
Vengono regolarmente eseguiti idonei backup, le copie di backup sono custodite coerentemente alla Policy per i backup.

Autenticazione e monitoraggio
Le attività, le eccezioni, gli errori e gli eventi relativi alla sicurezza delle informazioni da parte degli utenti del sistema e degli amministratori/operatori avvengono previo inserimento delle credenziali di autenticazione e adeguatamente protette. Gli orologi sono sincronizzati.

Controllo di software operativi
L'installazione di software sui sistemi operativi è controllata.

Gestione delle vulnerabilità tecniche
Le vulnerabilità tecniche sono corrette con idonee patch, e sono previste regole per l'installazione dei software da parte degli utenti. Applicazioni e sistemi operativi sono mantenuti aggiornati per risolvere vulnerabilità tecniche e correggere errori.

Considerazioni sull'audit per le informazioni di sistema
L'audit per l'area IT è programmato con regolarità annuale e controllato per minimizzare l'effetto avverso sui sistemi di produzione o l'accesso abusivo ai dati.

Sicurezza delle comunicazioni

Gestione della sicurezza della rete
Le reti e i servizi in rete sono resi sicuri, ad esempio attraverso la loro separazione.

Trasferimento delle informazioni
Sono previste policy, procedure ed accordi (ad es. accordi di riservatezza) relativi al trasferimento delle informazioni verso/da terze parti, compresi i messaggi elettronici.

Acquisizione, sviluppo e manutenzione del sistema

Requisiti di sicurezza dei sistemi di informazione
I requisiti per il controllo di sicurezza sono analizzati e specificati, comprese le applicazioni web e le transazioni.

Sicurezza nello sviluppo e processi di supporto
Le regole che governano la sicurezza dello sviluppo dei software/sistemi sono definite in una Policy. Le modifiche al sistema (sia per le applicazioni che per i sistemi operativi) sono controllate. I pacchetti software teoricamente non vengono modificati, e bisogna osservare i principi di sicurezza ingegneristica. L'ambiente di sviluppo viene reso sicuro e si controlla lo sviluppo esternalizzato. La sicurezza del sistema è testata regolarmente e sono definiti criteri di ammissibilità che includano gli aspetti di sicurezza.

Test di verifica dei dati
I test di verifica dei dati sono accuratamente selezionati e/o generati e controllati.

Rapporti con i fornitori

Sicurezza delle informazioni nei rapporti coi fornitori
Sono previste policy, procedure, sistemi di consapevolezza volti a proteggere le informazioni dell'organizzazione che siano accessibili ai soggetti esterni operanti nell'area IT e ad altri fornitori esterni per l'intera catena di fornitura, concordata nei contratti o negli accordi.

Gestione dei servizi resi dal fornitore
L'erogazione dei servizi resi dal fornitore è monitorata e rivista/verificata in relazione al contratto/accordo. Le modifiche al servizio sono controllate.

Gestione degli incidenti alle informazioni di sicurezza

Gestione degli incidenti sulla sicurezza delle informazioni e miglioramenti
Sono previste responsabilità e procedure (report, valutazioni, rispondere a e imparare da) volte a gestire in modo coerente ed efficace gli eventi, gli incidenti e le debolezze relative alla sicurezza delle informazioni, anche al fine di conservare prove valide in eventuali giudizi.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

Aspetti della sicurezza delle informazioni relativi alla continuità aziendale

Continuità della sicurezza delle informazioni
La continuità della sicurezza delle informazioni è pianificata, implementata e revisionata come parte integrante del sistema organizzativo di continuità aziendale.

Ridondanze
Le strutture IT sono sufficientemente ridondanti per soddisfare i requisiti di disponibilità.

Conformità

Conformità ai requisiti legali e contrattuali
L'organizzazione identifica e documenta i suoi obblighi alle autorità esterne e ad altre terze parti in relazione alla sicurezza delle informazioni, compresa la proprietà intellettuale, la documentazione contabile, le informazioni relative alla privacy/comunque idonee a consentire l'identificazione personale e la crittografia.

Revisione della sicurezza delle informazioni
I progetti dell'organizzazione relativamente alla sicurezza delle informazioni sono revisionati (verificati tramite audit) con modalità tali da garantire l'indipendenza della valutazione e rendicontate alla Direzione. I manager e il DPO revisionano
periodicamente la conformità dei dipendenti e dei sistemi alle policy di sicurezza, alle procedure, ecc., e promuovono azioni correttive ove necessario.

Con specifico riferimento al servizio MagNews SaaS ed in linea con quanto previsto dal previgente Allegato B al Codice in materia di protezione dei dati personali (D.lgs. 196/2003) e dall'art. 32 del GDPR, il Responsabile ha adottato fra l'altro le seguenti misure di sicurezza:

- implementazione di un sistema di autenticazione che attribuisce a ciascun utente credenziali proprie e riservate basate su codice identificativo e password;
- è possibile attivare in MagNews l'autenticazione 2FA e delle regole di blocco per indirizzo IP in modo da vincolare solo da specifici indirizzi IP l'accesso degli utenti al back-end, ai web services, ai servizi FTP e Simply SMTP della piattaforma.
- la password rispetta i seguenti requisiti:
  (a) deve essere composta da almeno 8 caratteri (la dimensione è configurabile fino ad un massimo di 50 caratteri); **(b)** non deve contenere il nome utente, e non può essere contenuta nel nome utente;
  (c) deve contenere almeno una lettera minuscola;
  (d) deve contenere almeno una lettera maiuscola;
  (e) deve contenere almeno un numero;
  (f) deve contenere almeno un carattere speciale tra: (_, -, $, £, %, #, &, !, ?, ^, +, *) e ha un periodo di scadenza configurato a 90 giorni;
- in caso di esigenza di recupero della password, l'utente riceve una e-mail contenente una password temporanea utilizzabile esclusivamente per il primo accesso all'interfaccia web della Piattaforma (c.d. "one time password"). Si precisa che il personale di Diennea non è in grado di recuperare la password, potendo unicamente eseguire il reset della stessa. Quando l'utente effettua il login con la password temporanea viene mostrata al medesimo una maschera nella quale l'utente deve inserire e successivamente confermare una nuova password, che non potrà comunque essere identica alla precedente;
- le password vengono trasmesse su canale cifrato con protocollo SSL e conservate cifrate con algoritmo di cifratura forte (AES256) all'interno di una specifica tabella;
- implementazione di un sistema di autorizzazione che, attraverso un sistema di profili, consente a ciascuna Persona Autorizzata, ovvero a classi omogenee di Persone Autorizzate, di poter trattare i dati compatibilmente con l'incarico svolto ed il ruolo ricoperto secondo i principi generali di liceità, correttezza, pertinenza e non eccedenza;
- tutte le interfacce di accesso e le pagine dell'applicazione sono rese sicure attraverso l'utilizzo di protocolli sicuri (HTTPS);
- Diennea garantisce la protezione da perdita e corruzione dei dati con una politica di backup giornaliera che prevede la copia dei dati e delle configurazioni su due diversi data center e la conservazione delle copie di backup per 60 giorni. Inoltre, è stato implementato un sistema di disaster recovery fra due diversi data center (geograficamente situati a circa 400km l'uno dall'altro) per garantire la continuità del servizio e dei dati. Tutte le operazioni di backup e disaster recovery sono disciplinate dal piano di business continuity aziendale (BCP). Tutti i dati archiviati o "at rest", come le copie di backup e di disaster recovery, sono conservati in maniera cifrata (con algoritmo forte AES256) e protetta;
- tutti i server che ospitano il servizio e tutti gli apparati elettronici utilizzati dal personale Diennea sono protetti contro eventuali tentativi di intrusione e/o attacco informatico da sistemi firewall, antivirus e DLP, sistemi IDS e HIDS e sono oggetto di continuo aggiornamento e hardening (secondo le linee guida CIS). Nel caso di utilizzo di apparati rimovibili e mobili questi vengono cifrati (full disk encryption) per mitigare i rischi da perdita involontaria o furto;
- tutti i sistemi di Diennea sono monitorati 24/7 contro minacce di attacco e comportamenti anomali e tutti gli accessi degli amministratori di sistema sono tracciati e conservati in maniera cifrata e non modificabile in conformità alla normativa vigente;
- il servizio viene erogato da sistemi ospitati presso i **data center TIM S.p.A. di Rozzano (MI) e Acilia (RM)**. Entrambe le già menzionate strutture risultano certificate ISO 9001:2015, ISO 14001 e ISO/IEC 27001:2013, garantiscono i più alti standard di resilienza fisica e logica e gestiscono la sicurezza fisica di accesso 24/7 attraverso personale dedicato e sistemi automatici di rilevamento e antintrusione: solo personale espressamente autorizzato può accedere direttamente ai sistemi Diennea;
- è previsto un programma continuo di formazione e aggiornamento del personale di Diennea sulle tematiche di sicurezza informatica e in materia di protezione dei dati personali;
- Diennea ha adottato una serie di Regolamenti Aziendali interni resi noti al proprio personale, che si è impegnato a garantire la riservatezza e sicurezza dei dati dei clienti di Diennea medesima;

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

▪ Diennea ha adottato e applica policy e procedure quali, a titolo esemplificativo:

- regole di utilizzo e scambio dei dati sia fra il personale dell'azienda da e per il cliente;
- regole di gestione degli apparati elettronici;
- regole di gestione della conclusione del contratto di lavoro con i dipendenti;
- controllo periodico di validità dei permessi delle utenze aziendali;
- Change Control Management Policy;
- Courtesy Security Notification Policy
- Incident Response and Notification Policy;
- Data Breach Response and Notification Policy;
- Development and Release Workflow Process.

▪ Diennea esegue periodicamente (con frequenza almeno annuale) attività di risk assessment, vulnerability assessment e penetration test e audit privacy al fine di verificare il livello di sicurezza e maturità della propria infrastruttura tecnologica e delle procedure adottate, nonché il livello di formazione del proprio personale.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

Allegato 3: Subresponsabili

L'Allegato 3, contenente l'elenco dei Subresponsabili impiegati dal Fornitore, è disponibile attraverso due modalità:

- al link https://www.diennea.com/lista-dei-subresponsabili/;
- previa richiesta scritta all'indirizzo e-mail dpo@diennea.com.

In caso di eventuali modifiche all'elenco condiviso in fase di sottoscrizione del presente Accordo per il Trattamento dei Dati, il Fornitore invierà una comunicazione all'Indirizzo E-mail di Notifica; dalla notifica del Fornitore decorre il termine di opposizione di cui alla Sezione 11.4(a) del Contratto che precede, restando inteso che è onere del Cliente consultare l'elenco aggiornato secondo le modalità di cui sopra.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com

Allegato 4: Istruzioni Aggiuntive

Le seguenti Istruzioni Aggiuntive integrano il presente Accordo per il Trattamento dei Dati:

1. *Istruzioni per gli Amministratori di Sistema - versione 1.0*
   - Il Fornitore si impegna a rispettare il Provvedimento dell'Autorità di Controllo denominato "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (e sue successive modifiche).
   - Il Fornitore si impegna a procedere alla redazione di una lettera di designazione individuale per ogni amministratore di sistema, successivamente alla valutazione dell'esperienza, della capacità e dell'affidabilità dei soggetti, contenente l'elencazione analitica degli ambiti di operatività.
   - Il Fornitore si impegna a procedere, con cadenza almeno annuale, ad un'attività di verifica degli amministratori di sistema, in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i Trattamenti dei Dati Personali previste dalle norme vigenti.
   - Il Fornitore si impegna a produrre, su richiesta del Cliente, la lista del personale designato quale amministratore di sistema recante l'elenco delle funzioni ad esso attribuite.
   - Il Fornitore si impegna ad implementare sistemi idonei alla registrazione degli accessi logici (log-in, log-out, tentativi di log-in e log-out) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Diennea S.r.l.

Viale G. Marconi 30/14 48018 Faenza (RA) – Italy Tel. (+39) 0546066100 Fax. (+39) 0546 399913
Altre sedi: Milano, Via Donatello 30 - Parigi, rue Meyerbeer 7
Capitale Sociale i.v. 111.495,65€ - P.Iva 02243600398

www.diennea.com