ALLEGATO A - DATA PROCESSING AGREEMENT (DPA)

## 1. DEFINIZIONI

Ai fini del presente DPA:

- **GDPR**: Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016.
- **Titolare**: Il Cliente che sottoscrive il Contratto e carica i propri dati sulla Piattaforma NOEVA, determinando finalità e mezzi del trattamento.
- **Responsabile**: 4D S.R.L. che tratta i dati personali per conto del Titolare nell'ambito dell'erogazione del servizio SaaS NOEVA.
- **Interessati**: Le persone fisiche i cui dati personali sono trattati (es. utenti finali, dipendenti clienti, contatti).
- **Dati Personali**: Qualsiasi informazione riguardante una persona fisica identificata o identificabile.
- **Trattamento**: Qualsiasi operazione sui dati personali (raccolta, registrazione, conservazione, consultazione, utilizzo, cancellazione, ecc.).
- **Violazione dei Dati Personali (Data Breach)**: Violazione di sicurezza che comporta distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali.

## 2. OGGETTO E DURATA

Il presente DPA disciplina il trattamento dei dati personali effettuato dal Responsabile per conto del Titolare nell'ambito dell'erogazione del servizio SaaS NOEVA.

Il trattamento avverrà nel rispetto del Regolamento (UE) 2016/679 ("GDPR") e della normativa nazionale applicabile in materia di protezione dei dati personali.

**Durata**: Il presente DPA ha efficacia per tutta la durata del contratto principale e permane per le obbligazioni di cui alla Sezione 9 (Restituzione/Cancellazione Dati) fino al loro completo adempimento.

## 3. NATURA E FINALITÀ DEL TRATTAMENTO

### 3.1 Tipologie di Dati Trattati

Il Responsabile può trattare le seguenti categorie di dati personali:

- Dati relativi al Titolare:
  - Dati anagrafici (nome, cognome, email, telefono)
  - Dati aziendali (ragione sociale, P.IVA, indirizzo sede)
  - Dati di utilizzo della piattaforma (log accessi, attività, preferenze)
  - Dati di fatturazione (coordinate bancarie, storico pagamenti)
- Dati relativi agli Utenti Finali (dipendenti/collaboratori del Titolare):
  - Dati anagrafici (nome, cognome, email aziendale)
  - Credenziali di accesso (username, hash password)
  - Dati di utilizzo della piattaforma
  - Eventuali dati business contenuti nei documenti/workspace gestiti
- Categorie particolari di dati (Art. 9 GDPR):



**4D S.R.L.**
CF/PI 03000790356 - R.E.A N. RE-331504 - Cap. Soc. 10.000,00 €
sede legale: Via Brigata Reggio 32 - 42124 - Reggio Emilia
sede operativa: Via Salvatore Viganò 2/A - 42124 - Reggio Emilia
email: info@gruppo4d.com - pec: 4DSRLPEC@legalmail.it

- NON sono previste categorie particolari di dati (dati sensibili su salute, opinioni politiche, dati biometrici, ecc.) salvo esplicita autorizzazione scritta del Titolare caso per caso.

### 3.2 Categorie di Interessati

- Dipendenti del Titolare
- Utenti nominativi della Piattaforma NOEVA
- Clienti, fornitori e altri soggetti i cui dati siano contenuti nei documenti caricati dal Titolare

### 3.3 Finalità del Trattamento

Il Responsabile tratta i dati personali esclusivamente per le seguenti finalità:

- Archiviazione documentale
- Organizzazione e indicizzazione dati
- Elaborazione semantica e generazione di embedding
- Elaborazione tramite modelli di Intelligenza Artificiale
- Gestione utenti e permessi
- Logging e sicurezza applicativa

**Il Responsabile NON può trattare i dati per finalità proprie, di marketing diretto, o per altri scopi non autorizzati dal Titolare.**

## 4. OBBLIGHI DEL RESPONSABILE

Il Responsabile si impegna a:

### 4.1 Istruzioni del Titolare

- Trattare i dati personali soltanto su istruzione documentata del Titolare, incluse eventuali istruzioni successive durante il periodo di validità del contratto.
- Informare immediatamente il Titolare se ritiene che un'istruzione violi il GDPR o altre disposizioni applicabili.

### 4.2 Riservatezza

- Garantire che le persone autorizzate al trattamento si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.
- Fornire formazione adeguata al personale sul GDPR e sulle misure di sicurezza.

### 4.3 Misure di Sicurezza Tecniche e Organizzative

Il Responsabile implementa e mantiene misure di sicurezza adeguate, incluse a titolo esemplificativo:



**4D S.R.L.**
CF/PI 03000790356 - R.E.A N. RE-331504 - Cap. Soc. 10.000,00 €
sede legale: Via Brigata Reggio 32 - 42124 - Reggio Emilia
sede operativa: Via Salvatore Viganò 2/A - 42124 - Reggio Emilia
email: info@gruppo4d.com - pec: 4DSRLPEC@legalmail.it

- **Misure Tecniche**:
  - Autenticazione forte (password complesse + 2FA dove disponibile)
  - Cifratura dei dati in transito (TLS 1.2+) e a riposo (AES-256 dove applicabile)
  - Controllo degli accessi basato su ruoli (least privilege)
  - Firewall e sistemi di rilevamento intrusioni
  - Antivirus e anti-malware aggiornati
  - Backup regolari cifrati
- **Misure Organizzative**:
  - Policy di sicurezza documentate
  - Gestione accessi (creazione, modifica, revoca)
  - Registro trattamenti ai sensi Art. 30 GDPR
  - Procedure di gestione incidenti
  - Audit periodici di sicurezza

## 4.4 Sub-Responsabili

**Autorizzazione generale**: Il Titolare autorizza in via generale il Responsabile a nominare sub-responsabili per l'erogazione del servizio SaaS NOEVA, ai sensi dell'Art. 28(2) GDPR. L'elenco dei sub-responsabili autorizzati alla data di sottoscrizione del presente DPA è riportato nella Sezione 4.5.

**Il Responsabile:**

- impone contrattualmente a ciascun sub-responsabile obblighi di protezione dei dati equivalenti a quelli previsti dal presente DPA;
- resta pienamente responsabile verso il Titolare per l'adempimento degli obblighi di ciascun sub-responsabile.

## 4.5 Sub-responsabili attuali autorizzati:

- Amazon Web Services (AWS)
  - Fornitore: Amazon Web Services EMEA SARL
  - Ruolo: Infrastruttura Cloud Provider
  - Finalità del trattamento:
    - Hosting
    - Database
    - Storage
    - infrastruttura AI (AWS Bedrock EU
    - networking e sicurezza
  - Localizzazione dati:
    - Regione Europea (es. eu-west-1 / EU region)
  - Categorie di dati potenzialmente trattati
    - Dati aziendali caricati in piattaforma
    - Dati personali contenuti nei documenti
    - Dati utenti piattaforma
    - Log applicativi
  - Garanzie:
    - Certificazioni ISO 27001
    - SOC 1 / SOC 2 / SOC 3
    - Conformità GDPR
    - Data Processing Addendum AWS
- Supabase Cloud



**4D S.R.L.**
CF/PI 03000790356 - R.E.A N. RE-331504 - Cap. Soc. 10.000,00 €
sede legale: Via Brigata Reggio 32 - 42124 - Reggio Emilia
sede operativa: Via Salvatore Viganò 2/A - 42124 - Reggio Emilia
email: info@gruppo4d.com - pec: 4DSRLPEC@legalmail.it

- Fornitore: Supabase Inc.
- Infrastruttura sottostante: Amazon Web Services (eu-west-1)
- Finalità del trattamento:
    - Database PostgreSQL
    - autenticazione utenti
    - storage oggetti
    - Row Level Security
- Localizzazione dati:
    - AWS eu-west-1 (Irlanda)
- Categorie di dati potenzialmente trattati:
    - Dati account utenti
    - Dati documentali
    - Metadati
    - Embedding vettoriali
    - Log tecnici
- Garanzie:
    - Data Processing Agreement Supabase
    - Hosting su AWS EU
    - Crittografia a riposo e in transito
    - Supabase Inc. è entità giuridica statunitense.
        - La residenza dei dati è configurata in regione AWS eu-west-1 (Irlanda, SEE).
        - Il trattamento avviene sulla base del DPA sottoscritto con Supabase Inc. e, ove applicabile, della certificazione del fornitore nell'ambito del EU-US Data Privacy Framework

- Redis Cloud
    - Fornitore: Redis Ltd.
    - Ruolo: utilizzato per dati volatili e temporanei, non per archiviazione persistente primaria.
    - Finalità del trattamento:
        - Caching temporaneo
        - gestione sessioni
        - ottimizzazione performance
    - Localizzazione dati:
        - Regione AWS EU (dati volatili, non archiviazione persistente)
    - Categorie di dati potenzialmente trattati
        - Token di sessione
        - Dati temporanei applicativi
        - Cache temporanea di query
    - Garanzie:
        - Crittografia in transito
        - Hosting su cloud provider europeo
        - Redis Ltd. è entità giuridica con sede negli Stati Uniti.
            - I dati volatili sono ospitati in regione AWS EU.
            - Il trattamento avviene sulla base del DPA sottoscritto con Redis Ltd. e, ove applicabile, della certificazione del fornitore nell'ambito del EU-US Data Privacy Framework.
- ClickHouse

- Fornitore: ClickHouse Inc.
- Infrastruttura: Amazon Web Services (eu-west-1)
- Ruolo: utilizzato per finalità di monitoraggio e analisi tecnica
- Finalità del trattamento :
    - Analisi dati
    - logging strutturato
    - monitoraggio
- Localizzazione dati:
    - AWS eu-west-1 (Irlanda)
- Categorie di dati potenzialmente trattati:
    - Log applicativi
    - Eventi di sistema
    - Dati aggregati di utilizzo
- Garanzie:
    - Hosting su AWS EU
    - Crittografia a riposo e in transito
    - ClickHouse Inc. è entità giuridica statunitense.
        - La residenza dei dati è configurata in regione AWS eu-west-1 (Irlanda, SEE).
        - Il trattamento avviene sulla base del DPA sottoscritto con ClickHouse Inc. e, ove applicabile, della certificazione del fornitore nell'ambito del EU-US Data Privacy Framework

- Sentry.io
    - Functional Software Inc. (Sentry)
    - Ruolo: Sentry è utilizzato per evitare l'inclusione non necessaria di dati personali nei log
    - Finalità del trattamento:
        - Monitoraggio errori applicativi
        - Debug tecnico
        - Log di crash
    - Localizzazione dati:
        - Data center UE (ove configurato)
    - Categorie di dati potenzialmente trattati:
        - Log di errore
        - Stack trace
        - Metadati tecnici
        - Eventuali dati applicativi inclusi nei log
    - Garanzie:
        - Data Processing Agreement Sentry
        - Crittografia in transito
        - Controlli accesso
        - Functional Software Inc. (Sentry) è entità giuridica statunitense.
            - La localizzazione dei dati è configurata in data center UE.
            - Il trattamento avviene sulla base del DPA sottoscritto con Sentry e, ove applicabile, della certificazione del fornitore nell'ambito del EU-US Data Privacy Framework.
            - Sentry è configurato per minimizzare la raccolta di dati personali nei log di errore (scrubbing automatico).

## 4.6 Misure di controllo sui Sub-Processor

Il responsabile:

- Verifica la conformità GDPR dei fornitori
- Sottoscrive DPA con ciascun Sub-processor
- Configura data residency in Regione Europea
- Applica principio di minimizzazione dei dati
- Limita l'accesso ai soli dati necessari

### 4.7 Aggiornamento elenco Sub-Processor

In caso di aggiunta o sostituzione di un Sub-responsabile, il Responsabile:

- **Notifica il Titolare** con almeno **15 giorni di preavviso** rispetto alla data prevista di inizio del trattamento da parte del nuovo Sub-responsabile, specificando: identità e sede legale del nuovo Sub-responsabile, finalità del trattamento, localizzazione dei dati e garanzie adottate.

- **Diritto di opposizione**: Il Titolare può opporsi alla nomina del nuovo Sub-responsabile entro **10 giorni** dalla ricezione della notifica, con motivazione scritta basata su ragioni oggettive relative alla protezione dei dati personali.

- **Gestione dell'opposizione**: In caso di opposizione motivata, le Parti si impegnano a negoziare in buona fede una soluzione alternativa entro 30 giorni. Se non si raggiunge un accordo, il Titolare ha facoltà di recedere dal contratto principale con effetto immediato, senza penali né costi aggiuntivi, con l'obbligo per il Responsabile di procedere alla restituzione o cancellazione dei dati ai sensi della Sezione 9.

- In assenza di opposizione entro il termine di cui al punto 2, il nuovo Sub-responsabile si intende autorizzato.

La notifica può avvenire tramite comunicazione email all'indirizzo indicato dal Titolare nella Sezione 14, oppure tramite pubblicazione dell'elenco aggiornato in un'area dedicata della piattaforma NOEVA, con contestuale notifica email al Titolare.

### 4.8 Assistenza al Titolare

Il Responsabile assiste il Titolare, tenuto conto della natura del trattamento:



**4D S.R.L.**
CF/PI 03000790356 - R.E.A N. RE-331504 - Cap. Soc. 10.000,00 €
sede legale: Via Brigata Reggio 32 - 42124 - Reggio Emilia
sede operativa: Via Salvatore Viganò 2/A - 42124 - Reggio Emilia
email: info@gruppo4d.com - pec: 4DSRLPEC@legalmail.it

A) **Richieste degli Interessati (Art. 15-22 GDPR)**:
- Diritto di accesso, rettifica, cancellazione, limitazione, portabilità, opposizione
- Il Responsabile risponde alle richieste entro 5 giorni lavorativi, fornendo i dati o le informazioni necessarie al Titolare per rispondere all'interessato

B) **Valutazione d'Impatto (DPIA - Art. 35 GDPR)**:
- Il Responsabile assiste il Titolare nella conduzione della DPIA, fornendo:
  i. informazioni dettagliate sulle caratteristiche del trattamento, sulle categorie di dati trattati e sulle misure di sicurezza adottate;
  ii. documentazione tecnica relativa all'architettura del servizio SaaS NOEVA, inclusi i flussi di dati, i modelli di Intelligenza Artificiale utilizzati (cfr. Sezione 6) e le modalità di elaborazione semantica e generazione di embedding;
  iii. descrizione delle misure tecniche e organizzative adottate per garantire la minimizzazione dei dati, la non riconducibilità degli embedding ai dati originali, e l'assenza di utilizzo dei dati per addestramento di modelli AI;
  iv. ogni altra informazione ragionevolmente necessaria al Titolare per valutare l'impatto del trattamento sui diritti e le libertà degli interessati.
- Il Responsabile fornisce la documentazione richiesta entro 15 giorni lavorativi dalla richiesta del Titolare.

C) **Consultazione Preventiva Autorità (Art. 36 GDPR)**:
- Collabora con il Titolare se necessario consultare l'Autorità Garante

## 4.9 Notifica Violazioni (Data Breach)

In caso di violazione dei dati personali, il Responsabile:

- **Notifica al Titolare entro 24 ore** dalla scoperta della violazione, tramite comunicazione all'indirizzo email indicato dal Titolare nella Sezione 14 del presente DPA.
- **Fornisce le seguenti informazioni**:
  - Natura della violazione (es. accesso non autorizzato, perdita dati, ecc.)
  - Categorie e numero approssimativo di interessati coinvolti
  - Categorie e numero approssimativo di registri di dati coinvolti
  - Probabili conseguenze della violazione
  - Misure adottate o proposte per porre rimedio e attenuare effetti negativi
- **Aggiornamenti successivi:** Qualora non sia possibile fornire tutte le informazioni di cui al punto 2 contestualmente alla notifica iniziale, il Responsabile le fornisce progressivamente senza ulteriore ritardo, e comunque entro 72 (settantadue) ore dalla scoperta della violazione, in modo da consentire al Titolare di ottemperare tempestivamente all'obbligo di notifica all'Autorità Garante ai sensi dell'Art. 33 GDPR**.**
- **Documenta ogni violazione** in un registro interno
- **Collabora con il Titolare** per eventuale notifica all'Autorità Garante (entro 72h) e agli interessati

## 4.10 Audit e Ispezioni

- Il Responsabile consente al Titolare (o revisore incaricato) di effettuare audit/ispezioni per verificare la conformità al DPA.
- Preavviso: almeno 15 giorni lavorativi (salvo urgenza in caso di data breach).
- Frequenza: massimo 1 audit all'anno (salvo fondato sospetto di violazione).
- Costi: a carico del Titolare, salvo accertamento violazioni gravi (costi a carico Responsabile).

## 4.11 DPO (Data Protection Officer)

Alla data di sottoscrizione del presente DPA, 4D S.R.L. non ha nominato un DPO ai sensi dell'Art. 37 GDPR, non ricorrendo i presupposti di cui alle lettere a), b) e c) del medesimo articolo. Il punto di contatto per le questioni relative alla protezione dei dati è raggiungibile all'indirizzo privacy@noeva.ai.



**4D S.R.L.**
CF/PI 03000790356 - R.E.A N. RE-331504 - Cap. Soc. 10.000,00 €
sede legale: Via Brigata Reggio 32 - 42124 - Reggio Emilia
sede operativa: Via Salvatore Viganò 2/A - 42124 - Reggio Emilia
email: info@gruppo4d.com - pec: 4DSRLPEC@legalmail.it

Qualora vengano meno le condizioni di esenzione, 4D S.R.L. provvederà alla nomina del DPO e ne darà comunicazione al Titolare.

## 5. TRASFERIMENTI INTERNAZIONALI

### 5.1 TRASFERIMENTI INTERNAZIONALI

Il Responsabile si impegna a:

- **NON trasferire dati personali al di fuori dello Spazio Economico Europeo (SEE)** senza previo consenso scritto del Titolare.
- In caso di trasferimento autorizzato, garantire che siano in atto adeguate garanzie ai sensi del Capo V del GDPR, tra cui a titolo esemplificativo: Clausole Contrattuali Standard della Commissione Europea (SCC, Decisione 2021/914/UE), decisioni di adeguatezza della Commissione Europea (incluso il EU-US Data Privacy Framework, Decisione del 10 luglio 2023), Binding Corporate Rules (BCR) approvate dall'Autorità competente, o altre garanzie adeguate previste dall'Art. 46 GDPR, eventualmente integrate da misure supplementari conformi alle Raccomandazioni 01/2020 dell'EDPB.
- Informare il Titolare sui Paesi destinatari e le garanzie applicate.

### 5.2 LOCAZIONE DATI

I dati personali sono ospitati in data center ubicati all'interno dello Spazio Economico Europeo (SEE), nella regione AWS eu-west-1 (Irlanda).

### 5.3 ACCESSO DA PAESI TERZI

Alcuni Sub-responsabili (cfr. Sezione 4.5) sono entità giuridiche stabilite negli Stati Uniti. Sebbene i dati risiedano fisicamente nel SEE, non è possibile escludere che personale tecnico di tali Sub-responsabili possa accedere ai dati da Paesi terzi per finalità di manutenzione, supporto tecnico o risoluzione incidenti. Tale accesso, ove configurabile come trasferimento ai sensi del Capo V del GDPR, avviene sulla base delle seguenti garanzie:

- Decisione di adeguatezza della Commissione Europea relativa al EU-US Data Privacy Framework (Decisione del 10 luglio 2023), per i Sub-responsabili certificati nell'ambito del DPF;
- Clausole Contrattuali Standard della Commissione Europea (SCC, Decisione 2021/914/UE), incorporate nei Data Processing Agreement sottoscritti con ciascun Sub-responsabile;
- Misure supplementari conformi alle Raccomandazioni 01/2020 dell'EDPB, tra cui: cifratura dei dati a riposo con chiavi gestite dal Responsabile o dal cloud provider europeo; politiche di accesso basate sul principio del least privilege; logging di tutti gli accessi ai dati personali.

### 5.4 PIANO DI CONTINGENZA

Qualora il EU-US Data Privacy Framework fosse invalidato o sospeso da un'autorità competente, il Responsabile si impegna a garantire la continuità delle garanzie di trasferimento attraverso le SCC già in essere e, ove necessario, ad adottare entro 30 giorni misure supplementari aggiuntive in linea con le indicazioni dell'EDPB o dell'Autorità Garante.

**Riepilogo garanzie cumulative per Sub-responsabili in Paesi terzi.** A titolo di sintesi e senza limitazione rispetto a quanto dettagliato nella Sezione 5.3, per ciascun Sub-responsabile stabilito in un Paese terzo il Responsabile garantisce il rispetto congiunto delle seguenti condizioni:

- residenza fisica dei dati personali in data center ubicati nel SEE;
- sottoscrizione di Data Processing Agreement contenente garanzie equivalenti al presente DPA;
- ove applicabile, certificazione del Sub-responsabile nell'ambito del EU-US Data Privacy Framework;



**4D S.R.L.**
CF/PI 03000790356 - R.E.A N. RE-331504 - Cap. Soc. 10.000,00 €
sede legale: Via Brigata Reggio 32 - 42124 - Reggio Emilia
sede operativa: Via Salvatore Viganò 2/A - 42124 - Reggio Emilia
email: info@gruppo4d.com - pec: 4DSRLPEC@legalmail.it

- adozione di misure supplementari (cifratura, pseudonimizzazione, controlli di accesso) conformi alle Raccomandazioni 01/2020 dell'EDPB.

Il venir meno di una o più delle condizioni sopra elencate per un Sub-responsabile comporta l'obbligo per il Responsabile di notificare tempestivamente il Titolare e di adottare le misure correttive di cui al primo comma della presente Sezione.

### 5.5 RICHIESTE DI ACCESSO DA AUTORITÀ DI PAESI TERZI

- Il Responsabile si impegna a informare tempestivamente il Titolare qualora riceva, direttamente o tramite un Sub-responsabile, una richiesta di accesso ai dati personali da parte di un'autorità pubblica di un Paese terzo (incluse richieste ai sensi del U.S. CLOUD Act, FISA o normative equivalenti), salvo che tale notifica sia espressamente vietata dalla legge applicabile.
- In caso di divieto legale di notifica, il Responsabile si impegna a compiere ogni sforzo ragionevole per contestare tale divieto e ottenere la possibilità di informare il Titolare.
- Il Responsabile non divulgherà dati personali in risposta a richieste di autorità di Paesi terzi, salvo che sia obbligato dalla legge applicabile, e in ogni caso valuterà preliminarmente se la richiesta è compatibile con il GDPR e con il diritto dell'Unione e degli Stati membri.
- Il Responsabile garantisce che i DPA sottoscritti con i Sub-responsabili stabiliti in Paesi terzi contengano clausole equivalenti a quelle del presente articolo.

## 6. UTILIZZO DI MODELLI DI INTELLIGENZA ARTIFICIALE

### 6.1 Infrastruttura AI

L'elaborazione tramite modelli di Intelligenza Artificiale avviene mediante il servizio Amazon Bedrock, nella regione europea (eu-west-1, Irlanda). I modelli AI utilizzati dalla Piattaforma NOEVA possono includere modelli di Anthropic (famiglia Claude), Amazon (famiglia Titan/Nova) e altri modelli disponibili su AWS Bedrock in regione europea.

Il Responsabile si riserva la facoltà di modificare, aggiornare o sostituire i modelli AI utilizzati, purché le garanzie di protezione dei dati di cui al presente articolo siano mantenute.

### 6.2 Flusso dei dati nelle elaborazioni AI

Nelle elaborazioni AI, il flusso dei dati è il seguente:

- Input: Porzioni di testo estratte dai documenti del Titolare, prompt dell'utente, e contestualizzazione da knowledge base (RAG) vengono inviati al modello AI tramite API di AWS Bedrock.
- Elaborazione: Il modello genera una risposta sulla base dell'input ricevuto.
- Output: La risposta viene restituita alla Piattaforma NOEVA e presentata all'utente.
- Nessuna persistenza presso il fornitore AI: Utilizzando AWS Bedrock con l'opzione di zero data retention attiva, i dati di input e output non vengono conservati da AWS o dal fornitore del modello AI al termine dell'elaborazione.

### 6.3 Garanzie sul trattamento AI

I dati personali trattati tramite modelli AI:

- Non vengono utilizzati per l'addestramento (training o fine-tuning) di modelli AI pubblici o di terzi. AWS Bedrock, nella configurazione adottata dal Responsabile, garantisce che i dati di input non vengano utilizzati per migliorare i modelli base;
- Non vengono condivisi con altri clienti di 4D o con terzi;

- Non vengono conservati dal fornitore AI oltre il tempo strettamente necessario all'elaborazione della singola richiesta;
- Non vengono riutilizzati dal Responsabile per finalità proprie, di profilazione, marketing o altre finalità non autorizzate dal Titolare.

### 6.4 Logging delle interazioni AI

Il Responsabile può conservare log delle interazioni AI (prompt e risposte) all'interno della Piattaforma NOEVA per le seguenti finalità:

- Funzionamento del servizio (storico conversazioni per l'utente);
- Debugging e risoluzione problemi tecnici;
- Monitoraggio qualità del servizio.

I log sono conservati nei sistemi del Responsabile all'interno del SEE e sono soggetti alle stesse misure di sicurezza e agli stessi termini di cancellazione dei Contenuti Cliente di cui alla Sezione 9.

### 6.5 Generazione di Embedding

Il Responsabile genera rappresentazioni vettoriali (embedding) dei documenti del Titolare per finalità di ricerca semantica e RAG. Gli embedding:

- Sono rappresentazioni numeriche non direttamente riconducibili al contenuto originale del documento;
- Sono conservati nel database della Piattaforma all'interno del SEE;
- Sono cancellati contestualmente alla cancellazione dei documenti originali o alla cessazione del contratto.

### 6.6 Conformità al Regolamento (UE) 2024/1689 (AI Act)

I sistemi di Intelligenza Artificiale integrati nella Piattaforma NOEVA sono classificati, allo stato attuale, come sistemi a **rischio limitato o minimo** ai sensi del Regolamento (UE) 2024/1689, in quanto utilizzati per finalità di assistenza all'elaborazione documentale, ricerca semantica e automazione di processi business, senza incidere direttamente su diritti fondamentali o su decisioni con effetti giuridici sugli interessati.

Il Responsabile si impegna a:

- Monitorare l'evoluzione della classificazione di rischio alla luce degli atti delegati e delle linee guida delle autorità competenti;
- Garantire la trasparenza sull'utilizzo di sistemi AI, in conformità con gli obblighi di cui all'Art. 50 del Regolamento (UE) 2024/1689;
- Aggiornare il presente DPA qualora la classificazione di rischio dei sistemi AI utilizzati dovesse mutare.

## 7. DIRITTI E OBBLIGHI DEL TITOLARE

Il Titolare:

- **Fornisce istruzioni chiare** al Responsabile sul trattamento dei dati.
- **Verifica la conformità** del Responsabile alle istruzioni e al GDPR.
- **Autorizza o rifiuta** l'uso di sub-responsabili.
- **Resta responsabile** del rispetto del GDPR per il trattamento complessivo.



**4D S.R.L.**
CF/PI 03000790356 - R.E.A N. RE-331504 - Cap. Soc. 10.000,00 €
sede legale: Via Brigata Reggio 32 - 42124 - Reggio Emilia
sede operativa: Via Salvatore Viganò 2/A - 42124 - Reggio Emilia
email: info@gruppo4d.com - pec: 4DSRLPEC@legalmail.it

## 8. RESPONSABILITÀ E RISARCIMENTO

### 8.1 Responsabilità verso Interessati

Ai sensi Art. 82 GDPR:

- Il Titolare e il Responsabile sono responsabili in solido per i danni causati agli interessati da trattamenti non conformi al GDPR.
- Il Responsabile è esonerato da responsabilità se dimostra che l'evento dannoso non gli è imputabile.

### 8.2 Azioni di Rivalsa

- Se il Titolare viene chiamato a risarcire l'interessato per violazioni imputabili al Responsabile, il Titolare ha diritto di rivalsa integrale nei confronti del Responsabile.
- Il Responsabile tiene indenne il Titolare da sanzioni amministrative dell'Autorità Garante derivanti da inadempimenti del Responsabile.

### 8.3 Limitazione di Responsabilità

a) Le limitazioni di responsabilità previste nel contratto principale (cap di responsabilità) **NON si applicano** a:

- Violazioni dolose o gravemente colpose del GDPR da parte del Responsabile.
- Sanzioni dell'Autorità Garante imputabili al Responsabile.
- Risarcimenti a interessati per violazioni GDPR imputabili al Responsabile.

b) Per tutti gli altri casi di responsabilità derivanti dal presente DPA non rientranti nella lettera a), la responsabilità complessiva del Responsabile è limitata a un importo pari al corrispettivo annuo versato dal Titolare per il servizio SaaS NOEVA nei 12 mesi precedenti l'evento, al netto dei consumi di NOEVA Token e spazio disco utilizzato, con un minimo di Euro 1.000,00 e un massimo di Euro 10.000,00.

c) Le limitazioni di cui alla lettera b) non si applicano in caso di violazione degli obblighi di riservatezza (Sezione 4.2) o di trasferimento non autorizzato di dati al di fuori del SEE (Sezione 5).



**4D S.R.L.**
CF/PI 03000790356 - R.E.A N. RE-331504 - Cap. Soc. 10.000,00 €
sede legale: Via Brigata Reggio 32 - 42124 - Reggio Emilia
sede operativa: Via Salvatore Viganò 2/A - 42124 - Reggio Emilia
email: info@gruppo4d.com - pec: 4DSRLPEC@legalmail.it

## 9. RESTITUZIONE E CANCELLAZIONE DEI DATI

Alla cessazione del contratto principale, il Responsabile, a scelta del Titolare:

- **Restituzione**:
  - Restituisce tutti i dati personali al Titolare in formato strutturato, di uso comune e leggibile da dispositivo automatico (es. CSV, JSON, XML).
  - Termine: entro 30 giorni dalla cessazione (o termine diverso concordato).
- **Cancellazione:**
  - Cancella in modo sicuro e irreversibile tutti i dati personali e le copie esistenti, salvo obbligo legale di conservazione.
  - Termine: entro 60 giorni dalla cessazione (o termine diverso concordato).
  - Fornisce attestazione scritta dell'avvenuta cancellazione.
- **Cancellazione presso Sub-responsabili:**
  - Il Responsabile provvede a richiedere ai Sub-responsabili la cancellazione dei dati personali del Titolare entro i termini previsti dai rispettivi DPA.
  - Il Responsabile fornisce al Titolare, su richiesta, conferma dell'avvenuta cancellazione presso i Sub-responsabili, ove tale conferma sia ottenibile secondo i termini contrattuali in essere con i medesimi.

**Eccezioni**: Il Responsabile può conservare i dati nella misura e per il periodo richiesto dalla legge (es. obblighi fiscali, conservazione documentale), informando il Titolare e limitando il trattamento alla sola conservazione.

## 10. REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Il Responsabile mantiene per iscritto un registro di tutte le categorie di attività di trattamento svolte per conto del Titolare, contenente:

- Nome e dati di contatto del Responsabile e di eventuali sub-responsabili
- Categorie di trattamenti effettuati per conto del Titolare
- Categorie di interessati e di dati personali
- Trasferimenti internazionali (se applicabili)
- Misure di sicurezza tecniche e organizzative

Il registro è messo a disposizione dell'Autorità Garante su richiesta.

## 11. COOPERAZIONE CON AUTORITÀ DI CONTROLLO

Il Responsabile coopera con l'Autorità Garante per la Protezione dei Dati Personali per qualsiasi questione relativa al trattamento dei dati, su richiesta della stessa o del Titolare.



**4D S.R.L.**
CF/PI 03000790356 - R.E.A N. RE-331504 - Cap. Soc. 10.000,00 €
sede legale: Via Brigata Reggio 32 - 42124 - Reggio Emilia
sede operativa: Via Salvatore Viganò 2/A - 42124 - Reggio Emilia
email: info@gruppo4d.com - pec: 4DSRLPEC@legalmail.it

## 12. MODIFICHE AL DPA

Il Responsabile può proporre modifiche al presente DPA esclusivamente per adeguamento a nuove disposizioni normative o regolamentari applicabili, a provvedimenti dell'Autorità Garante, o a decisioni di autorità giudiziarie competenti.

Le modifiche proposte sono comunicate al Titolare con preavviso di almeno **60 giorni** rispetto alla data di efficacia, indicando le disposizioni oggetto di modifica e le ragioni normative che le rendono necessarie.

Il Titolare può comunicare il proprio dissenso entro **30 giorni** dalla ricezione della comunicazione. In caso di dissenso, le Parti si impegnano a negoziare in buona fede. Se non si raggiunge un accordo entro ulteriori 30 giorni, il Titolare ha facoltà di recedere dal contratto principale senza penali, con obbligo di restituzione o cancellazione dei dati ai sensi della Sezione 9.

In assenza di comunicazione di dissenso entro il termine, le modifiche si intendono accettate dal Titolare.

## 13. DISPOSIZIONI FINALI

- Il presente DPA è parte integrante del contratto principale.
- In caso di contrasto tra DPA e contratto principale, prevale il DPA per quanto attiene alla protezione dati personali.
- Legge applicabile: legge italiana e GDPR.
- Foro competente: come da contratto principale.

## 14. CONTATTI DATA PROTECTION

**Responsabile (4D S.R.L.)**:

- Indirizzo: via Viganò 2, 42124 Reggio Emilia (RE)
- Email privacy: privacy@noeva.ai
- PEC: 4dsrlpec@legalmail.it

**Titolare (Cliente):**

- Nome: [da compilare]
- Indirizzo: [da compilare]
- Email privacy: [da compilare]
- PEC: [da compilare]
- DPO (se nominato): [da compilare]

## SOTTOSCRIZIONE

**Per il Fornitore - 4D S.R.L.**

| | |
|---|---|
| **Sede Legale** | via Brigata Reggio 32, 42124 Reggio Emilia (RE) |
| **Sede Operativa** | via Viganò 2, 42124 Reggio Emilia (RE) |
| **P.IVA** | 03000790356 |
| **PEC** | 4dsrlpec@legalmail.it |
| **Amministratore Delegato** | Dosi Alessandro |
| **Nato il** | 01/09/1977 a Montecchio Emilia (RE) |
| **Codice Fiscale** | DSOLSN77P01F463W |

Firma Legale Rappresentante: _____ Data: _____

**Per il Cliente - [AZIENDA]**

| | |
|---|---|
| **Sede Legale** | [da compilare] |
| **Sede Operativa** | [da compilare] |
| **P.IVA** | [da compilare] |
| **PEC** | [da compilare] |
| **Ambito di Specializzazione** | [da compilare] |
| **Amministratore Delegato** | [da compilare] |
| **Nato il** | [da compilare] |
| **Codice Fiscale** | [da compilare] |

Firma Legale Rappresentante: _____ Data: _____



**4D S.R.L.**
CF/PI 03000790356 - R.E.A N. RE-331504 - Cap. Soc. 10.000,00 €
sede legale: Via Brigata Reggio 32 - 42124 - Reggio Emilia
sede operativa: Via Salvatore Viganò 2/A - 42124 - Reggio Emilia
email: info@gruppo4d.com - pec: 4DSRLPEC@legalmail.it