



DPA – DATA PROCESSING AGREEMENT

Appendice GDPR al Contratto di Utilizzo del Servizio DoQEngine

Ultimo aggiornamento: 19/11/2025

Tra:

Cliente (di seguito: "Titolare")

e

Stabilidea Srl, P.IVA 05389850263, sede in VIA DON GIOVANNI GATTOLI 16 - 31036 - ISTRANA (TV),

(di seguito: "Responsabile")

congiuntamente "Parti".

1. Oggetto del DPA

Il presente Data Processing Agreement ("DPA") disciplina il trattamento dei dati personali effettuato da Stabilidea Srl in qualità di **Responsabile del Trattamento** ai sensi dell'art. 28 GDPR, esclusivamente per l'erogazione del servizio **DoQEngine**.

DoQEngine elabora documenti forniti dal Titolare (PDF, immagini, scansioni) per convertirli in JSON, XML, MD o altri formati strutturati.

Il Titolare rimane l'unico soggetto a decidere **finalità e mezzi** del trattamento dei dati contenuti nei documenti.

2. Ruoli e responsabilità

- Il **Titolare** determina finalità e mezzi del trattamento dei dati personali contenuti nei documenti caricati.
- Il **Responsabile** tratta tali dati solo per eseguire le attività tecniche richieste dal Titolare, senza finalità proprie.

Il Responsabile **non legge, analizza o utilizza** i contenuti per scopi diversi dall'elaborazione tecnica.

3. Tipologia di dati e interessati

3.1 Dati trattati

I documenti caricati dal Titolare possono contenere:

- dati identificativi
- dati fiscali e contabili
- dati di contatto

- dati presenti in fatture, scontrini, DDT, conferme d'ordine, rapportini, estratti conto, contratti, documenti commerciali o altre tipologie di documenti
- altri dati personali presenti nel documento fornito dal Titolare

Il Responsabile non conosce preventivamente la natura dei dati contenuti nei documenti.

3.2 Categorie particolari di dati

Il Titolare **si impegna a non inviare** dati appartenenti alle categorie particolari ex art. 9 GDPR o dati relativi a reati, salvo che disponga di idonea base giuridica.

Il Titolare si assume ogni responsabilità per il caricamento di dati non conformi.

4. Finalità del trattamento

Il Responsabile tratta i dati **solo** per:

- eseguire l'elaborazione documentale
- generare l'output richiesto (JSON/XML/MD/altri formati strutturati)
- archiviare file e output su storage Cloud NIS2 compliant
- fornire accesso tramite API e dashboard
- garantire funzionamento, sicurezza e continuità del servizio
- eseguire log tecnici limitati ai metadati

Il Responsabile **non**:

- utilizza i dati per addestrare modelli
- effettua analisi, profilazioni o indicizzazioni dei contenuti
- accede volontariamente ai dati salvo richiesta tecnica del Titolare

5. Durata del trattamento

Il trattamento avviene per tutta la durata del contratto o finché il Titolare utilizza DoQEngine.

6. Sub-responsabili (Sub-processors)

Il Titolare autorizza l'uso dei seguenti sub-responsabili:

6.1 Provider USA per elaborazione documentale

Il Responsabile si avvale di un provider di terze parti situato negli **Stati Uniti**, che riceve **il contenuto integrale dei documenti** per eseguire l'estrazione OCR e la conversione.

Il trasferimento avviene tramite:

- Clausole Contrattuali Standard (SCC), ove applicabili
- impostazioni che escludono l'uso dei dati per training dei modelli

6.2 Infrastruttura e storage

- **Cubbit S3 – storage in area UE (eu-central-1)**

- **OVH (EU)** – infrastruttura server e hosting

Il Responsabile mantiene una lista aggiornata dei sub-responsabili.

Il Titolare accetta l'uso di tali fornitori.

7. Trasferimenti extra-UE

Poiché i dati vengono inviati negli Stati Uniti per l'elaborazione documentale:

- il Titolare **autorizza esplicitamente** il trasferimento ai sensi dell'art. 49(1)(a) GDPR
- comprende e accetta i rischi connessi al trasferimento in un Paese privo di decisione di adeguatezza
- solleva il Responsabile da responsabilità derivanti da comportamenti del provider terzo fuori dal suo controllo

8. Sicurezza dei dati (art. 32 GDPR)

Il Responsabile implementa misure tecniche e organizzative adeguate, tra cui:

- cifratura TLS/HTTPS
- storage su Cubbit S3 con sicurezza conforme NIS2
- segregazione logica tra tenant
- accesso interno controllato e tracciato
- audit log dei job
- infrastruttura su server in UE (OVH)
- autenticazione OAuth o Magic Link
- monitoraggio di sicurezza e controlli manuali

Il Responsabile può aggiornare le misure tecniche per migliorare il livello di protezione.

9. Log e metadati

I log del servizio non contengono il contenuto dei documenti ma solo:

- fileKey
- job_id
- timestamp
- stato del job
- errori tecnici
- informazioni necessarie all'erogazione del servizio

10. Conservazione e cancellazione dei dati

Il Responsabile conserva documenti e output **senza scadenza automatica**.

Il Titolare può richiedere cancellazione **in qualsiasi momento** tramite email su supporto durevole.

Il Responsabile procederà alla cancellazione entro tempi ragionevoli.

11. Violazioni dei dati personali (Data Breach)

Il Responsabile:

- adotterà misure immediate per ridurre l'impatto
- informerà il Titolare se un incidente potrebbe aver compromesso dati trattati per suo conto
- fornirà informazioni utili per eventuali notifiche all'Autorità o agli interessati (obblighi del Titolare)

12. Assistenza al Titolare

Il Responsabile assisterà il Titolare:

- nel rispondere a richieste degli interessati
- nel garantire misure di sicurezza
- nella gestione di richieste dell'Autorità Garante

Tale assistenza può essere soggetta a costi aggiuntivi per richieste complesse.

13. Audit

Il Titolare può richiedere informazioni sulla sicurezza del servizio.

Eventuali audit formali o ispezioni devono essere:

- programmati con almeno 20 giorni di preavviso
- limitati alle aree pertinenti
- eseguiti senza interferire con l'operatività
- soggetti a costi aggiuntivi se superano ragionevole impegno

14. Responsabilità

Il Titolare:

- è responsabile dei dati personali contenuti nei documenti che carica
- garantisce la liceità dei dati e delle operazioni
- indennizza il Responsabile in caso di uso illecito, improvvisto o non conforme

Il Responsabile risponde solo:

- nei limiti del contratto principale
- entro il massimale previsto (importo dei crediti acquistati nel mese dell'incidente)

15. DPA personalizzati

Il Titolare può richiedere:

- **DPA custom**
- **SLA personalizzati**

entrambi soggetti ad accordo separato.

16. Termine del contratto

Alla cessazione del rapporto:

- il Responsabile interrompe ogni elaborazione
- su richiesta del Titolare, cancella file e output
- i log tecnici non contenenti dati personali possono essere conservati per sicurezza e audit

17. Legge applicabile e foro competente

Il presente DPA è regolato dalla legge italiana.

Il foro competente esclusivo è Treviso.