ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI (DPA)

ai sensi dell'art. 28 del Regolamento (UE) 2016/679 — Allegato A alle Condizioni Generali di Contratto "Legale Offline" (Servizio Pro)

Versione 2.0 del 16/07/2026

1. Parti, premesse e ambito

1.1. Il presente accordo ("DPA") è concluso tra l'Utente del Servizio Pro delle Condizioni Generali "Legale Offline" (il "Titolare" o, ove l'Utente agisca a sua volta quale responsabile per conto dei propri clienti, il "Responsabile primario") e Quality & Safety s.r.l., Via L. Einaudi n. 38, Moncalieri (TO), C.F./P.IVA 10018310010 (il "Responsabile" o "Fornitore"). Esso disciplina i trattamenti di dati personali effettuati dal Responsabile per conto del Titolare nell'ambito delle sole Funzionalità Cloud del Servizio Pro di cui all'art. 19 delle Condizioni Generali (schede di analisi, Sintesi, conversazioni IA nei Fascicoli).

1.2. Il DPA costituisce parte integrante delle Condizioni Generali (Allegato A), è efficace dall'attivazione del Servizio Pro e resta in vigore per la durata del contratto principale. In caso di contrasto sul trattamento dei dati, prevale il presente DPA.

1.3. Il DPA non si applica: (i) al Servizio Base e alla fase locale di pseudonimizzazione del Servizio Pro, in cui il Fornitore non effettua alcun trattamento (artt. 5 e 14-15 delle Condizioni Generali); (ii) ai dati di account, log e fatturazione dell'Utente, dei quali il Fornitore è autonomo titolare (Informativa privacy del Sito).

1.4. Le Parti si danno atto che le funzionalità di IA del Servizio Pro costituiscono un sistema di IA a rischio minimo ai sensi del Regolamento (UE) 2024/1689 (AI Act), per le ragioni esposte all'art. 19.7 delle Condizioni Generali: non ricorrono pratiche vietate (art. 5 AI Act) né ipotesi di alto rischio (art. 6 e Allegato III, in particolare punto 8 sull'amministrazione della giustizia, riferito ai sistemi usati da o per conto dell'autorità giudiziaria); lo strumento opera come ausilio documentale sotto piena supervisione umana del professionista, senza decisioni con effetti giuridici su persone fisiche; gli obblighi di trasparenza ex art. 50 AI Act sono assolti mediante l'informazione all'Utente e il contrassegno dei contenuti generati.

2. Oggetto, natura, finalità e durata del trattamento

Elemento	Descrizione
Oggetto	Elaborazione, tramite modelli di IA eseguiti su Amazon Bedrock, del testo pseudonimizzato trasmesso dall'Utente nell'ambito delle Funzionalità Cloud (generazione di sintesi, indici, timeline, report di qualità e risposte conversazionali sul documento pseudonimizzato)
Natura delle operazioni	Raccolta temporanea, elaborazione automatizzata, restituzione dell'output, cancellazione; nessuna scrittura su storage durevole (v. art. 6)
Finalità	Esclusivamente l'erogazione delle Funzionalità Cloud richieste dall'Utente
Durata	Pari alla durata del contratto principale (abbonamento Pro)
Categorie di interessati	Clienti, controparti, terzi e altri soggetti menzionati negli atti e documenti dell'Utente
Categorie di dati	Dati personali comuni eventualmente residui nel testo pseudonimizzato

Elemento	Descrizione
	(identificativi indiretti non riconosciuti o non revisionati); in via eventuale e non voluta, categorie particolari (art. 9 GDPR) e dati relativi a condanne e reati (art. 10 GDPR), tipici degli atti legali, ove non correttamente pseudonimizzati dall'Utente

3. Istruzioni del Titolare

3.1. Il Responsabile tratta i dati soltanto su istruzione documentata del Titolare; l'istruzione si intende impartita mediante l'utilizzo delle Funzionalità Cloud secondo la documentazione del Servizio. Il Responsabile informa il Titolare qualora ritenga che un'istruzione violi il GDPR o altre disposizioni applicabili.

3.2. Il Responsabile non utilizza i dati per finalità proprie e non li utilizza né consente che siano utilizzati per l'addestramento, la messa a punto o il miglioramento di modelli di intelligenza artificiale, propri o di terzi. Tale garanzia è assicurata a valle mediante la configurazione di Amazon Bedrock di cui all'art. 6.2: i contenuti trattati non sono accessibili ai fornitori dei modelli né utilizzati da AWS per l'addestramento.

4. Riservatezza

Il Responsabile garantisce che le persone autorizzate al trattamento si sono impegnate alla riservatezza o sono soggette a un adeguato obbligo legale di segretezza e che l'accesso ai dati è limitato a quanto strettamente necessario all'erogazione delle Funzionalità Cloud e alla gestione tecnica del Servizio.

5. Misure di sicurezza (art. 32 GDPR)

Il Responsabile adotta le misure tecniche e organizzative descritte nell'Appendice 1, tra cui: pseudonimizzazione a monte del testo trattato (unico contenuto trasmesso); cifratura in transito (TLS 1.2 o superiore, raccomandato TLS 1.3) e a riposo; minimizzazione (i dati sono trattati per il solo tempo necessario all'elaborazione e non conservati oltre la restituzione dell'output); controllo degli accessi e autenticazione; registrazione degli eventi; gestione delle vulnerabilità.

6. Sub-responsabili

6.1. Il Titolare autorizza in via generale il ricorso a sub-responsabili. L'elenco vigente è riportato nell'Appendice 2; il sub-responsabile principale è Amazon Web Services EMEA SARL ("AWS"), per il servizio Amazon Bedrock.

6.2. Configurazione di Amazon Bedrock. Il Responsabile si impegna a mantenere la seguente configurazione, dalla quale il presente DPA dipende: (i) elaborazione in regione europea; (ii) modalità di conservazione dei dati impostata su "zero data retention" (data_retention_mode: none): nessun dato di richiesta o risposta è scritto su storage durevole di AWS né condiviso con i fornitori dei modelli; (iii) impiego esclusivo di modelli che supportano tale modalità, con esclusione dei modelli che richiedono la condivisione dei dati con il fornitore (provider data share); (iv) applicazione della configurazione mediante policy tecniche (IAM/SCP) che impediscono modifiche non autorizzate della modalità di conservazione. In tale configurazione, i fornitori dei modelli non

hanno accesso ai prompt e agli output: i modelli sono eseguiti in account di distribuzione gestiti da Amazon Bedrock, ai quali i fornitori non hanno accesso.

6.3. Il Responsabile informa il Titolare di ogni modifica prevista (aggiunta o sostituzione di sub-responsabili, cambio di regione, modifica della modalità di conservazione) con preavviso di 15 giorni, dando al Titolare la possibilità di opporsi; in caso di opposizione motivata, il Titolare può recedere dalle sole Funzionalità Cloud, con rimborso dei Crediti IA non consumati. Il Responsabile impone a ciascun sub-responsabile obblighi equivalenti a quelli del presente accordo e resta pienamente responsabile verso il Titolare del loro operato.

7. Trasferimenti extra-UE

7.1. L'elaborazione avviene in regione europea. Eventuali trasferimenti verso paesi terzi nell'ambito dei servizi AWS (ivi inclusi accessi di supporto dagli Stati Uniti) avvengono sulla base della decisione di adeguatezza UE-USA (EU-U.S. Data Privacy Framework, cui Amazon Web Services, Inc. ha aderito) e, in via sussidiaria, delle clausole contrattuali standard della Commissione (Decisione UE 2021/914) incorporate nel Data Processing Addendum di AWS, integrate ove necessario da misure supplementari all'esito di valutazione d'impatto sul trasferimento (TIA). I riferimenti sono riportati nell'Appendice 2.

7.2. Il Responsabile non attiva funzionalità di inferenza cross-region verso regioni extra-UE.

8. Assistenza al Titolare

Il Responsabile, tenuto conto della natura del trattamento, assiste il Titolare con misure tecniche e organizzative adeguate: (i) nel dare seguito alle richieste di esercizio dei diritti degli interessati (artt. 15-22 GDPR), inoltrando senza ingiustificato ritardo ogni richiesta eventualmente ricevuta direttamente; si osserva che, non conservando il Responsabile alcun contenuto oltre l'elaborazione, l'esercizio dei diritti si svolge di regola presso il Titolare; (ii) negli adempimenti di cui agli artt. 32-36 GDPR (sicurezza, notifica delle violazioni, DPIA e consultazione preventiva), fornendo le informazioni in proprio possesso, inclusa la documentazione tecnica sulla configurazione di cui all'art. 6.2.

9. Violazioni di dati personali

Il Responsabile notifica al Titolare, senza ingiustificato ritardo e comunque entro 48 ore dal momento in cui ne ha avuto conoscenza, ogni violazione di dati personali che riguardi i trattamenti oggetto del presente accordo, fornendo le informazioni di cui all'art. 33, par. 3, GDPR e cooperando alle attività di contenimento e rimedio.

10. Audit

Il Responsabile mette a disposizione del Titolare le informazioni necessarie a dimostrare il rispetto degli obblighi dell'art. 28 GDPR e consente e contribuisce ad attività di revisione, comprese ispezioni, condotte dal Titolare o da altro soggetto incaricato, con preavviso di almeno 15 giorni, in orario lavorativo, al massimo una volta l'anno salvo violazioni accertate o richieste dell'autorità, nel rispetto della riservatezza dei sistemi e dei dati di altri clienti. In prima istanza, gli obblighi di audit possono essere soddisfatti mediante: (i) le certificazioni del Responsabile (ISO 9001, ISO/IEC 27001, 27017, 27018); (ii) le certificazioni e i report di audit indipendenti di AWS (ISO/IEC 27001, 27017,

27018, SOC 1/2/3, C5), resi disponibili tramite AWS Artifact; (iii) la documentazione della configurazione di cui all'art. 6.2.

11. Cancellazione e restituzione

In ragione dell'architettura del Servizio, i dati trattati nelle Funzionalità Cloud non sono conservati oltre l'elaborazione e la restituzione dell'output: non vi è pertanto, di regola, alcun dato da restituire o cancellare al termine della prestazione. Al termine del contratto il Responsabile attesta per iscritto, su richiesta del Titolare, l'assenza di conservazione di contenuti, salvi gli obblighi di conservazione previsti dal diritto dell'Unione o nazionale (che non riguardano i contenuti documentali).

12. Responsabilità e disposizioni finali

12.1. Ciascuna parte risponde dei danni causati dal trattamento nei termini dell'art. 82 GDPR.

12.2. Per quanto non previsto si applicano le Condizioni Generali; legge applicabile e foro sono quelli ivi indicati (legge italiana, Foro di Torino).

Appendice 1 — Misure tecniche e organizzative

- Contenuto trattato: esclusivamente testo pseudonimizzato a monte sul dispositivo dell'Utente (pseudonimi del tipo [PERSONA_1]); mai documenti originali o dizionari.
- Cifratura in transito: TLS 1.2 o superiore su tutte le tratte (client → piattaforma → Amazon Bedrock); raccomandato TLS 1.3.
- Cifratura a riposo: applicata da AWS alle componenti di servizio; nessuna persistenza dei contenuti di inferenza nella configurazione "zero data retention".
- Controllo accessi: autenticazione del personale autorizzato, principio del minimo privilegio (IAM), autenticazione a più fattori sulle utenze amministrative.
- Policy tecniche di enforcement: policy IAM/SCP che vietano la modifica della modalità di conservazione dei dati verso valori diversi da "none".
- Registrazione eventi: log delle attività API (senza contenuti dei prompt) e monitoraggio di sicurezza.
- Gestione vulnerabilità: aggiornamenti di sicurezza, hardening, test periodici.
- Organizzazione: designazione degli autorizzati ex art. 29 GDPR, istruzioni scritte, formazione periodica, procedure di gestione delle violazioni con notifica in 48 ore.

Appendice 2 — Sub-responsabili e trasferimenti

Sub-responsabile	Servizio	Sede / luogo del trattamento	Garanzie per il trasferimento
Amazon Web Services EMEA SARL	Amazon Bedrock — elaborazione IA dei testi pseudonimizzati	Lussemburgo; elaborazione in regione europea	AWS GDPR Data Processing Addendum; EU-U.S. Data Privacy Framework (Amazon Web Services, Inc.); SCC Decisione UE 2021/914; TIA documentata

Sub-responsabile	Servizio	Sede / luogo del trattamento	Garanzie per il trasferimento
Amazon Web Services EMEA SARL	Infrastruttura della piattaforma	Lussemburgo; elaborazione in regione europea	AWS GDPR Data Processing Addendum; EU-U.S. Data Privacy Framework (Amazon Web Services, Inc.); SCC Decisione UE 2021/914; TIA documentata

Riferimenti: documentazione AWS su protezione dei dati e conservazione dei dati in Amazon Bedrock (docs.aws.amazon.com/bedrock — sezioni "Data protection" e "Data retention"); AWS GDPR Center; AWS Artifact per certificazioni e report di audit.