

Accordo sul Trattamento dei Dati Personali

Data Processing Agreement — Allegato ai Termini di Servizio REVISIO, ai sensi dell'art. 28 del Regolamento (UE) 2016/679 (GDPR)

Ultimo aggiornamento: 26-10-2026

Premesse

- Il presente Accordo sul Trattamento dei Dati (di seguito, l'“Accordo”) integra e forma parte inscindibile dei Termini di Servizio del Servizio REVISIO (di seguito, i “Termini”), e si applica automaticamente a ogni Utente che attiva un Account, incluso il Piano Trial gratuito.
- Nell'ambito dell'utilizzo del Servizio, l'Utente carica, genera e tratta documenti e informazioni (bilanci, carte di lavoro, rilievi, verbali) che possono contenere dati personali riferiti a persone fisiche terze (es. titolari di ditte individuali, soci, amministratori, dipendenti delle società oggetto di revisione).
- Con riferimento a tali dati, l'Utente agisce quale Titolare autonomo del trattamento, mentre Rosario Costanzo (di seguito, il “Responsabile”) agisce quale Responsabile del trattamento ai sensi dell'art. 28 GDPR, nei limiti e alle condizioni di cui al presente Accordo.

1. Definizioni

Ai fini del presente Accordo si applicano le definizioni di cui all'art. 4 del Regolamento (UE) 2016/679 (“GDPR”), e in particolare: “Dati Personali”, “Trattamento”, “Titolare del trattamento”, “Responsabile del trattamento”, “Interessato”, “Violazione dei dati personali”. Con “Dati del Cliente” si intendono, ai fini del presente Accordo, i dati personali contenuti nei documenti e nelle informazioni che l'Utente carica o genera utilizzando il Servizio.

2. Ruoli delle parti

Le parti danno atto che, con riferimento ai Dati del Cliente:

- l'Utente è Titolare del trattamento, in quanto determina le finalità e i mezzi del trattamento dei dati personali contenuti nei documenti caricati nel Servizio;
- il Responsabile tratta i Dati del Cliente esclusivamente per conto e su istruzione documentata dell'Utente, nei limiti necessari a fornire le funzionalità del Servizio (conservazione, organizzazione, visualizzazione, elaborazione tecnica dei documenti caricati), secondo quanto previsto dai Termini e dal presente Accordo.

3. Oggetto, natura e finalità del trattamento

Il Responsabile tratta i Dati del Cliente al solo fine di erogare il Servizio, e in particolare per: conservazione dei documenti caricati; organizzazione e visualizzazione dei dati all'interno delle

funzionalità del Servizio (incarichi, trimestri, carte di lavoro, rilievi, bozze e verbali); esecuzione di backup e misure di continuità operativa; assistenza tecnica su richiesta dell'Utente. Il dettaglio del trattamento è riportato nell'Allegato 1.

4. Durata del trattamento

Il trattamento ha durata pari a quella del rapporto contrattuale tra le parti (Termini di Servizio) e cessa, salvo diverso obbligo di legge, al termine del periodo di esportazione dati di 30 giorni successivo alla cessazione dell'abbonamento, previsto alla Sezione 14 dei Termini, decorso il quale il Responsabile procede alla cancellazione definitiva dei Dati del Cliente secondo quanto previsto dalla medesima Sezione 14 dei Termini.

5. Tipologia di dati personali e categorie di interessati

Categoria di interessati	Tipologie di dati personali eventualmente trattati
Titolari di ditte individuali, soci, amministratori delle società oggetto di revisione	Nome, cognome, codice fiscale, dati contenuti in bilanci e documenti contabili
Dipendenti delle società oggetto di revisione	Nome, cognome, dati relativi a retribuzioni/TFR nella misura in cui compaiono nei documenti contabili caricati
Utenti dello Studio (Account del Cliente)	Nome, cognome, email, ruolo all'interno dello Studio

6. Obblighi del Responsabile del trattamento

Ai sensi dell'art. 28, par. 3, GDPR, il Responsabile:

- tratta i Dati del Cliente soltanto su istruzione documentata dell'Utente, anche in relazione ai trasferimenti di dati personali verso un paese terzo, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile; in tal caso il Responsabile informa l'Utente circa tale obbligo giuridico prima del trattamento, salvo che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- garantisce che le persone autorizzate a trattare i Dati del Cliente si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adotta tutte le misure richieste ai sensi dell'art. 32 GDPR (sicurezza del trattamento), come descritte nell'Allegato 3;
- rispetta le condizioni di cui ai paragrafi 2 e 4 dell'art. 28 GDPR per il ricorso a un altro responsabile del trattamento (sub-responsabile), secondo quanto previsto alla Sezione 7;

- e) tenuto conto della natura del trattamento, assiste l'Utente con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo dell'Utente di dare seguito alle richieste per l'esercizio dei diritti dell'interessato (artt. 15-22 GDPR);
- f) assiste l'Utente nel garantire il rispetto degli obblighi di cui agli artt. 32-36 GDPR (sicurezza del trattamento, notifica delle violazioni, valutazione d'impatto, consultazione preventiva), tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile;
- g) su scelta dell'Utente, cancella o restituisce tutti i Dati del Cliente dopo la cessazione del rapporto, secondo quanto previsto alla Sezione 4, e cancella le copie esistenti salvo che il diritto dell'Unione o nazionale preveda la conservazione dei dati;
- h) mette a disposizione dell'Utente tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dall'Utente o da un altro soggetto da questi incaricato, nei limiti e con le modalità di cui alla Sezione 11.

7. Sub-responsabili del trattamento

L'Utente autorizza in via generale il Responsabile a ricorrere a sub-responsabili del trattamento per l'erogazione del Servizio, nei limiti indicati nell'Allegato 2. Il Responsabile impone a ciascun sub-responsabile, tramite contratto scritto, obblighi di protezione dei dati personali non meno rigorosi di quelli previsti dal presente Accordo, e resta pienamente responsabile nei confronti dell'Utente dell'adempimento degli obblighi del sub-responsabile.

Il Responsabile informa l'Utente di eventuali modifiche previste relative all'aggiunta o sostituzione di sub-responsabili, dando così all'Utente l'opportunità di opporsi a tali modifiche entro 15 giorni dalla comunicazione, per motivi legittimi legati alla protezione dei propri dati.

8. Trasferimenti extra-UE

Qualora il trattamento dei Dati del Cliente comporti un trasferimento di dati personali al di fuori dello Spazio Economico Europeo (SEE), tale trasferimento avviene nel rispetto delle garanzie previste dal Capo V del GDPR (decisione di adeguatezza, Clausole Contrattuali Standard, o altre garanzie adeguate), come più specificamente descritto nella Privacy Policy del Servizio, qui richiamata. Resta fermo quanto precisato alla Sezione 5.1 della Privacy Policy e alla Sezione 9.1 dei Termini di Servizio in merito all'elaborazione tramite Google Gemini, non riconducibile al Responsabile.

9. Violazioni dei dati personali

Il Responsabile notifica all'Utente, senza ingiustificato ritardo e comunque entro 48 ore dal momento in cui ne viene a conoscenza, ogni violazione dei Dati del Cliente di cui sia venuto a conoscenza, fornendo le informazioni ragionevolmente disponibili per consentire all'Utente di adempiere ai propri obblighi di notifica ai sensi degli artt. 33 e 34 GDPR.

10. Misure di sicurezza tecniche e organizzative

Il Responsabile adotta le misure di sicurezza tecniche e organizzative descritte nell'Allegato 3, e si impegna a mantenerle adeguate all'evoluzione dello stato dell'arte, ai costi di attuazione, alla natura, all'oggetto, al contesto e alle finalità del trattamento, nonché al rischio per i diritti e le libertà delle persone fisiche.

11. Audit e verifica

L'Utente può richiedere, con un preavviso ragionevole non inferiore a 15 giorni e non più di una volta all'anno (salvo motivate ragioni, incluse istruzioni di un'autorità di controllo), informazioni e documentazione a dimostrazione del rispetto degli obblighi del presente Accordo. Eventuali verifiche in loco sono concordate tra le parti con ragionevole anticipo e condotte in modo da minimizzare l'impatto sull'operatività del Responsabile e sulla sicurezza degli altri Utenti del Servizio.

12. Responsabilità

Ciascuna parte è responsabile dei danni causati dal trattamento effettuato in violazione del GDPR e del presente Accordo, nei limiti e secondo le modalità previste dall'art. 82 GDPR e dalla Sezione 16 dei Termini di Servizio, qui richiamata.

13. Durata e cessazione dell'Accordo

Il presente Accordo ha efficacia per tutta la durata dei Termini di Servizio e si estingue automaticamente alla loro cessazione, fatto salvo quanto previsto alla Sezione 4 in merito al periodo di conservazione post-cessazione e alle disposizioni che per loro natura sono destinate a sopravvivere (riservatezza, responsabilità).

14. Legge applicabile e foro competente

Il presente Accordo è disciplinato dalla legge italiana. Per ogni controversia relativa alla validità, interpretazione, esecuzione o risoluzione del presente Accordo si applica quanto previsto alla Sezione 19 dei Termini di Servizio.

Allegato 1. Dettaglio del trattamento

Elemento	Descrizione
Oggetto del trattamento	Conservazione ed elaborazione tecnica dei documenti e dei dati caricati dall'Utente nel Servizio REVISIO
Durata	Per tutta la durata del rapporto contrattuale, come da Sezione 4

Elemento	Descrizione
Natura del trattamento	Raccolta, registrazione, conservazione, organizzazione, consultazione, elaborazione tecnica, cancellazione
Finalità	Erogazione del Servizio secondo i Termini di Servizio sottoscritti dall'Utente
Categorie di interessati	Vedi Sezione 5
Categorie di dati personali	Vedi Sezione 5

Allegato 2. Elenco dei sub-responsabili del trattamento

Sub-responsabile	Servizio fornito	Localizzazione del trattamento
Hetzner, UE	Hosting e conservazione dei dati e del Software	Germania (SEE)
Register.it	Servizio di posta elettronica e comunicazioni	Italia (SEE)
Stripe Payments Europe Ltd	Gestione dei pagamenti e della fatturazione ricorrente	Stati Uniti

Nota: l'elaborazione tramite Google Gemini non è inclusa in questo elenco, per le ragioni esposte alla Sezione 5.1 della Privacy Policy e alla Sezione 9.1 dei Termini di Servizio.

Allegato 3. Misure di sicurezza tecniche e organizzative

- Cifratura dei dati in transito (connessioni HTTPS/TLS) e, ove applicabile, a riposo.
- Autenticazione individuale degli utenti con credenziali personali e gestione dei ruoli e permessi di accesso (titolare, revisore, collaboratore, sindaco, amministratore).
- Isolamento logico dei dati tra i diversi Utenti/Studi (architettura multi-tenant).
- Backup periodici e procedure di ripristino dei dati.

- Le API Key Gemini fornite dagli Utenti vengono conservate cifrate nel database (cifratura a riposo), con la chiave di cifratura mantenuta separatamente dall'infrastruttura di archiviazione dei dati. L'accesso alla API Key in chiaro è limitato al solo processo automatizzato che la utilizza per inoltrare la richiesta a Google Gemini per conto dell'Utente: nessuna interfaccia amministrativa, log applicativo o altro componente del Servizio consente la visualizzazione della API Key in chiaro da parte del personale del Responsabile.
- Registrazione (log) degli accessi e delle operazioni rilevanti ai fini di sicurezza, con esclusione sistematica di API Key e altre credenziali dal contenuto dei log.
- In caso di sospetta violazione dei dati personali trattati tramite il Servizio, il Responsabile segue la seguente procedura interna: (i) la persona che rileva o riceve segnalazione dell'incidente ne dà immediata comunicazione al Titolare dell'attività (Rosario Costanzo), che assume la gestione dell'incidente; (ii) entro 24 ore dalla rilevazione viene effettuata una prima valutazione della natura dell'incidente, dei dati coinvolti e del rischio per gli interessati; (iii) se la valutazione conferma una violazione di dati personali, viene data notifica all'Utente/Titolare del trattamento interessato entro il termine di cui alla Sezione 9; (iv) l'incidente viene documentato per iscritto (data, natura, dati coinvolti, misure adottate), a prescindere dall'obbligo di notifica, ai fini del registro delle violazioni eventualmente richiesto dalla normativa applicabile.