

Accordo sul Trattamento dei Dati Personali ai sensi dell Articolo 28 GDPR

sia.solutions di Carraretto Andrea | P.IVA 04506580283 | PEC sia.solutions@pec.it Versione 1.4 | Aggiornato al 12/01/2026

Accordo standard: documentare negli allegati i trattamenti, le misure effettive e i subresponsabili prima del trattamento, anche richiamando documenti pertinenti già completi e consegnati. Non occorre ricopiare le condizioni standard.

Il presente accordo regola il trattamento di dati personali che sia.solutions di Carraretto Andrea svolge per conto del Cliente nell'esecuzione dei servizi acquistati. Il Cliente opera come Titolare oppure, se responsabile per un diverso titolare, conferma di essere autorizzato alla nomina; ruoli e istruzioni sono identificati nell'allegato individuale.

1 Parti oggetto e durata

1.1 Responsabile: sia.solutions di Carraretto Andrea, P.IVA 04506580283, C.F. CRRNDR88S28G224T. Contatti privacy e incidenti: info@siasolutions.it e sia.solutions@pec.it. L'indirizzo della sede è riportato all'art. 1 delle Condizioni Generali di Fornitura dei Servizi, documento 01. Titolare/Cliente, referente e contatti: come identificati nell'Ordine e nell'allegato individuale.

1.2 Oggetto, natura, finalità, categorie di interessati, tipi di dati e istruzioni sono descritti nell'allegato A, da documentare prima del trattamento, anche mediante rinvio a un allegato pertinente già completo, identificato e consegnato al Cliente. Non occorre ricopiare condizioni standard o informazioni già documentate; restano necessarie le informazioni effettive richieste per il trattamento. L'accordo dura per l'esecuzione del servizio e le successive operazioni autorizzate di restituzione e cancellazione. Non autorizza finalità diverse dal servizio o trasferimenti indiscriminati.

1.3 Per dati amministrativi trattati dal Fornitore per finalità proprie si applica l'Informativa Privacy; tali trattamenti sono distinti da quelli per conto del Cliente. Se il Cliente è responsabile, le istruzioni e autorizzazioni del titolare originario devono essere coerenti con questo incarico.

2 Istruzioni e obblighi del Cliente

2.1 Il Responsabile tratta i dati soltanto su istruzioni documentate, anche per trasferimenti fuori dello SEE, salvo obbligo di legge cui è soggetto: in tal caso informa preventivamente il Cliente, salvo divieto normativo per rilevanti motivi di interesse pubblico. L'Ordine, le configurazioni autorizzate e le richieste registrate costituiscono istruzioni nei limiti del servizio.

2.2 Il Cliente determina finalità e basi giuridiche, fornisce informative, gestisce autorizzazioni e dati pertinenti e comunica esigenze particolari. Dati particolari, giudiziari o trattamenti ad alto rischio richiedono preventiva identificazione e verifica delle misure; non si presume che un piano standard sia adeguato a ogni rischio.

2.3 Il Responsabile informa immediatamente il Cliente se ritiene che un'istruzione violi il GDPR o altre disposizioni applicabili, e richiede chiarimenti. Non assume decisioni ulteriori sulle finalità del trattamento né riutilizza i dati per pubblicità o finalità proprie incompatibili.

3 Persone autorizzate e sicurezza

3.1 Accessi sono limitati a persone autorizzate per necessità di servizio, soggette a riservatezza contrattuale o legale e istruzioni. Il Fornitore può autorizzare collaboratori persone fisiche nell'ambito della propria organizzazione secondo ruoli e bisogno effettivo; un operatore distinto che tratta per suo conto è invece subresponsabile e segue l'art. 4.

3.2 Il Responsabile adotta misure tecniche e organizzative adeguate al rischio ai sensi dell'art. 32 GDPR, descritte nell'allegato B e verificate prima dell'attivazione. Sono valutati controllo degli accessi, protezione delle credenziali, aggiornamenti, isolamento, protezione dei trasferimenti, backup, ripristino, gestione di incidenti e verifica delle misure. Nessuna specifica misura è dichiarata già presente se non verificata nell'allegato.

3.3 Il Cliente applica le misure di propria competenza e comunica rischi o incidenti. La ripartizione non elimina gli obblighi inderogabili del Responsabile. Cambi di misure non riducono arbitrariamente il livello di protezione concordato e sono documentati secondo il rischio.

4 Subresponsabili e trasferimenti

4.1 Il Cliente concede autorizzazione generale scritta all'impiego dei subresponsabili nominativamente identificati nell'allegato C, con funzione, dati, paesi e garanzie. Nessun soggetto è autorizzato da un elenco vuoto o da un generico riferimento a fornitori. Il Responsabile mantiene e consegna l'elenco aggiornato.

4.2 Nuovi subresponsabili o sostituzioni sono comunicati al Cliente con almeno 15 giorni di anticipo rispetto all'accesso ai dati, consentendo opposizione motivata su protezione dei dati. Le parti cercano una soluzione compatibile; se non disponibile, il trattamento interessato non viene affidato al soggetto contestato e si concordano modifica o cessazione della componente senza pregiudicare i diritti legali. Per un cambiamento che non possa attendere occorre un'autorizzazione specifica scritta prima dell'affidamento.

4.3 Il Responsabile impone al subresponsabile obblighi sostanzialmente equivalenti a quelli richiesti dall'art. 28 GDPR e resta pienamente responsabile verso il Cliente dell'adempimento degli obblighi del subresponsabile. Autorizzazione e subaffidamento non esonerano il Fornitore.

4.4 Infrastruttura primaria e copie europee sono collocate secondo la scheda. Servizi di archiviazione aggiuntivi possono comportare trasferimenti o accessi fuori dello SEE solo dopo verifica del piano, della controparte contrattuale, dei paesi e del meccanismo del capo V GDPR, con eventuali valutazioni e misure supplementari. Garanzie e istruzioni sono documentate nell'allegato C prima del trasferimento; non basta la dichiarazione commerciale dell'operatore.

5 Assistenza diritti e violazioni

5.1 Il Responsabile assiste il Cliente, con misure adeguate alla natura del trattamento, per richieste degli interessati e obblighi degli artt. 32-36 GDPR, comprese sicurezza, valutazioni d'impatto e consultazioni preventive, tenendo conto delle informazioni disponibili. Richieste ricevute dagli interessati sono inoltrate al Cliente; non vengono decise autonomamente salvo incarico valido o obbligo di legge.

5.2 Dopo aver avuto conoscenza di una violazione di dati personali, il Responsabile informa il Cliente senza ingiustificato ritardo ai contatti indicati. Comunica, anche progressivamente se necessario, natura dell'evento, dati e interessati coinvolti ove noti, conseguenze probabili, misure adottate e contatto operativo. Non attende il completamento di un'indagine per dare il primo avviso.

5.3 Il Responsabile collabora a contenimento, recupero e documentazione. Il Cliente valuta notifiche all'autorità e agli interessati nei termini applicabili, salvo diverso incarico e obblighi propri del Responsabile. Non è pattuito un termine che consenta di ritardare l'avviso fino a 72 ore.

5.4 Attività supplementari fuori dal perimetro ordinario possono essere quotate preventivamente nei limiti consentiti, senza subordinare l'assistenza dovuta per legge al pagamento né addebitare automaticamente la gestione di violazioni imputabili al Responsabile.

6 Informazioni verifiche e audit

6.1 Il Responsabile mette a disposizione le informazioni necessarie a dimostrare il rispetto dell'art. 28 e consente e contribuisce ad audit e ispezioni del Cliente o di un soggetto incaricato, secondo modalità proporzionate al rischio e rispettose dei dati di altri clienti.

6.2 Le verifiche ordinarie sono coordinate con preavviso ragionevole e riservatezza; si possono usare prima evidenze documentali adeguate, senza sostituire o impedire il diritto di audit. Preavviso e limiti organizzativi non operano quando incompatibili con un incidente, richiesta dell'autorità o altro obbligo inderogabile. Eventuali costi ragionevoli aggiuntivi sono concordati senza impedire le verifiche dovute.

7 Restituzione cancellazione e responsabilità

7.1 Al termine il Responsabile, a scelta del Cliente, restituisce o cancella i dati e cancella le copie, salvo obbligo di legge. Le finestre di recupero contrattuali e legali sono rispettate. Il Cliente comunica la scelta; il Responsabile la sollecita prima della cancellazione e, in assenza di istruzioni dopo la finestra applicabile e l'avviso, procede alla cancellazione prevista, salvo obblighi contrari.

7.2 Le copie residue non immediatamente eliminabili sono isolate dall'uso ordinario, protette e cancellate alla rotazione entro la retention massima di 30 giorni dalla creazione. Non sono conservate indefinitamente. Un eventuale ripristino tecnico durante tale periodo riapplica le istruzioni di cancellazione; il Responsabile informa delle modalità e conferma la cancellazione su richiesta.

7.3 Restano i diritti degli interessati, dell'autorità e la responsabilità prevista dal GDPR. I limiti B2B delle Condizioni Generali non riducono obblighi inderogabili di protezione dati né i diritti riconosciuti dalla legge. In caso di contrasto, questo accordo prevale per il trattamento svolto per conto del Cliente.

8 Allegato A — Descrizione individuale del trattamento

Le clausole dell'accordo si applicano nella versione standard; eventuali deroghe richiedono accordo espresso nei limiti di legge. I dati dei presenti allegati descrivono il trattamento effettivo e non sono semplici variazioni facoltative: devono essere documentati prima del trattamento. È possibile rinviare a documenti già completi, pertinenti, identificati per versione e consegnati al Cliente, senza ricopiare dati o condizioni standard. Misure e operatori comuni possono essere descritti in schede comuni applicabili al servizio; eventuali differenze specifiche devono essere indicate. Un campo vuoto non sostituisce informazioni necessarie mancanti.

Ordine / servizio e versione dell'allegato: _____

Cliente, referente privacy e recapiti per richieste o incidenti: _____

Ruolo del Cliente: ☐ Titolare del trattamento ☐ Responsabile per un altro titolare autorizzato alla nomina. Eventuale titolare originario e riferimento all'autorizzazione:

Servizi e componenti oggetto del trattamento: _____

Natura e finalità: conservazione, consultazione tecnica autorizzata, trasmissione, backup, ripristino e cancellazione nei limiti dei servizi acquistati. Eventuali ulteriori attività espressamente autorizzate: _____

Categorie di interessati, ad esempio dipendenti, clienti o utenti dell'applicazione: _____

Tipi di dati personali trattati: _____

Dati particolari o giudiziari: ☐ Assenti, dopo verifica dell'ambito ☐ Presenti, descritti nell'allegato seguente: _____

Rischi specifici ed esigenze di protezione comunicati dal Cliente: _____

Durata del trattamento e riferimento alla durata del servizio: _____

Istruzioni documentate del Cliente e attività autorizzate: _____

Scelta e modalità di restituzione / cancellazione, secondo le finestre contrattuali e legali: _____

9 Allegato B — Misure effettive, backup e conservazione

Descrivere le sole misure effettivamente adottate per il servizio. Un campo vuoto non attesta una misura presente né l'adeguatezza al rischio: le misure pertinenti devono essere verificate e documentate prima del trattamento. La descrizione può richiamare una scheda comune identificata per versione e consegnata al Cliente.

Scheda delle misure allegata, versione e data di verifica: _____

Accessi, autorizzazioni, privilegi e protezione delle credenziali: _____

Protezione dei dati in transito e a riposo, compresa l'eventuale cifratura effettiva: _____

Aggiornamenti, separazione dei clienti e protezione delle componenti: _____

Log, monitoraggio, gestione degli incidenti e verifiche delle misure: _____

Dati coperti dalle copie, frequenza effettiva e componenti: _____

Per le app soggette al documento 06 sono previsti backup giornalieri e settimanali dei dati dell'applicazione conservati nell'ambiente gestito. Per ogni servizio restano da indicare in questo allegato l'ambito pertinente e le destinazioni effettive. La conservazione massima delle copie è di 30 giorni dalla creazione.

Destinazioni delle copie e soggetti autorizzati all'accesso, con rinvio all'allegato C: _____

Rotazione e cancellazione delle copie: _____

Verifiche delle copie e test di ripristino effettivamente previsti: _____

Modalità di ripristino e riferimento alle condizioni del servizio: _____

Il ripristino è gestito dal Fornitore. Per le app del documento 06 è a pagamento nei limiti e con le salvaguardie di quel documento. Non è garantito ogni punto di ripristino salvo accordo specifico, senza deroga all'esecuzione diligente delle attività incluse. Non si presume un programma di test, una misura di cifratura o un'autenticazione aggiuntiva in assenza di verifica.

10 Allegato C — Subresponsabili e garanzie

Elenco individuale consegnato al Cliente, versione e data: _____

Compilare una scheda per ciascun operatore giuridicamente distinto che tratta dati per conto del Responsabile. L'elenco vuoto non autorizza subresponsabili. Se non ne sono impiegati, indicare espressamente «nessuno» dopo verifica. Ulteriori operatori sono riportati in schede allegate con gli stessi campi.

Denominazione legale e identificazione del soggetto: _____

Ruolo, funzione e servizio affidato: _____

Dati personali e categorie di interessati coinvolti: _____

Paesi di conservazione e di accesso ai dati: _____

Durata dell'incarico e accordo ai sensi dell'art. 28 GDPR: _____

Eventuali ulteriori subaffidamenti e condizioni applicabili: _____

Trasferimenti fuori dello SEE: ☐ Non previsti, dopo verifica ☐ Previsti secondo le garanzie documentate di seguito: _____

Meccanismo di trasferimento, valutazioni e misure supplementari pertinenti, con riferimento alla documentazione consegnata: _____

Il nome commerciale di un operatore non è necessario nelle condizioni commerciali pubbliche generali, ma l'identità dei subresponsabili deve essere concretamente conoscibile nell'allegato individuale prima del trattamento. Categorie generiche o dichiarazioni commerciali di conformità non sostituiscono l'elenco, gli accordi e le garanzie richiesti.

11 Accettazione

Il Cliente e il Responsabile accettano il presente accordo versione 1.4 e gli allegati A, B e C completati, identificati dalla seguente versione/data: _____.

Cliente e Ordine: _____

Data e firma del Cliente: _____

Data e firma del Responsabile: _____