ConduCodice · Nomina a responsabile del trattamento

Allegato al Contratto quadro, ai sensi dell'art. 28 del Regolamento (UE) 2016/679 (GDPR).

Ruoli e trattamenti

Art. 1. Ruoli

1.1 Il Cliente è titolare del trattamento dei dati personali inseriti nel Software. Con la firma del Contratto quadro nomina il Fornitore responsabile del trattamento.

1.2 La nomina vale per i software ospitati sui server del Fornitore e per gli accessi di assistenza autorizzati dal Cliente. Non vale per i software che il Cliente gestisce da sé dopo il Riscatto o dopo l'ultima rata del Leasing.

1.3 Il Fornitore è titolare autonomo dei dati che tratta per gestire il rapporto contrattuale, la fatturazione e l'Area Clienti, secondo la propria informativa privacy.

1.4 I termini con la maiuscola hanno il significato del Contratto quadro. In caso di contrasto sulla protezione dei dati personali prevale questo documento, salvo per il limite di responsabilità.

Art. 2. Trattamenti affidati

Voce	Contenuto
Oggetto	Ospitalità, conservazione, backup, ripristino, protezione del Software e, in modalità ACS, elaborazione dei dati
Finalità	Erogare il Software e i servizi previsti dal Contratto, secondo le istruzioni del Cliente
Durata	Quella del Contratto, più i tempi dell'art. 13
Dati personali	Quelli che il Cliente inserisce nel Software, indicati nel Preventivo, oltre a dati tecnici e di sicurezza
Interessati	Dipendenti, collaboratori, clienti e fornitori del Cliente e altri utenti del Software
Luogo	Server del Fornitore in Italia, salvo quanto previsto dall'Allegato A

2.1 Dati sensibili (art. 9 GDPR), dati giudiziari (art. 10 GDPR) e dati di minori sono ammessi solo se dichiarati prima nel Preventivo e accettati dal Fornitore, che può chiedere un corrispettivo aggiuntivo e istruzioni specifiche.

2.2 Il Cliente garantisce di avere una base giuridica per i trattamenti e di aver informato gli interessati. Decide da solo finalità, contenuti e tempi di conservazione dei dati nel Software. È suo l'adempimento delle regole sul controllo dei lavoratori, se il Software le riguarda.

Regole del trattamento

Art. 3. Istruzioni

3.1 Il Fornitore tratta i dati solo su istruzione documentata del Cliente. Sono istruzioni il Contratto, questo documento, le impostazioni del Software e le richieste scritte accettate dal Fornitore.

3.2 Istruzioni nuove che richiedono attività non previste sono a pagamento, previa stima scritta. Il Fornitore tratta i dati in altro modo solo se la legge lo impone, avvisando il Cliente quando è consentito.

3.3 Se ritiene che un'istruzione violi la normativa, il Fornitore avvisa il Cliente e può sospenderla. Non ha l'obbligo di una verifica legale delle istruzioni.

Art. 4. Riservatezza

Chi tratta i dati per conto del Fornitore è vincolato alla riservatezza e riceve istruzioni adeguate.

Art. 5. Sicurezza

5.1 Il Fornitore adotta le misure dell'Allegato B e può aggiornarle, senza ridurre il livello complessivo di protezione. Il Cliente le ha valutate e le ritiene adeguate ai trattamenti dichiarati.

5.2 Se i trattamenti cambiano, ad esempio con nuovi dati sensibili, il Cliente avvisa prima il Fornitore, e le parti concordano eventuali misure aggiuntive a pagamento.

5.3 Il Cliente è responsabile della sicurezza di dispositivi, utenti, credenziali, codici OTP e chiave manuale di recupero, come previsto dall'art. 20 del Contratto quadro.

Art. 6. Accessi del Fornitore

6.1 L'accesso di assistenza avviene solo su autorizzazione del Cliente dall'Area Clienti, per ciò che sceglie e per il tempo che sceglie, da 1 ora a 7 giorni, revocabile in ogni momento. Ogni accesso è registrato e il Cliente può scaricarne il report firmato.

6.2 Il Fornitore può intervenire senza autorizzazione preventiva solo per proteggere i sistemi durante un incidente di sicurezza o per eseguire un ripristino di emergenza. Se l'intervento riguarda il Software del Cliente, lo avvisa entro 24 ore. L'intervento non comporta la lettura dei dati riservati, salvo quanto previsto dall'art. 20.3 del Contratto quadro per la modalità ACS.

6.3 Il Fornitore non può reimpostare gli accessi del Cliente.

6.4 Per l'assistenza il Fornitore può usare software di controllo remoto dei terminali del Cliente, solo su richiesta o con il consenso del Cliente per ogni sessione. Il Fornitore annota data, durata e motivo della sessione, e non copia dati fuori dal terminale, salvo istruzione del Cliente. Durante la sessione può vedere ciò che appare sullo schermo. Il Cliente chiude ciò che non vuole mostrare e informa i propri lavoratori.

Art. 7. Sub-responsabili

7.1 Il Cliente autorizza in via generale i sub-responsabili dell'Allegato A e quelli nuovi comunicati dal Fornitore.

7.2 Il Fornitore comunica i nuovi sub-responsabili con 15 giorni di preavviso, salvo urgenze di sicurezza. Il Cliente può opporsi entro quel termine per motivi concreti legati alla protezione dei dati.

7.3 Se le parti non trovano una soluzione, il Cliente può recedere dal servizio interessato senza penali, e questo è il suo unico rimedio. Restano dovute le somme maturate.

7.4 Il Fornitore impone ai sub-responsabili obblighi di protezione dei dati adeguati. Risponde del loro operato verso il Cliente nei limiti dell'art. 14.

7.5 I fornitori di servizi scelti dal Cliente, compresi quelli collegati con chiavi API del Cliente, non sono sub-responsabili del Fornitore. Il loro rapporto con il Cliente è regolato dai rispettivi termini.

Art. 8. Trasferimenti fuori dallo Spazio economico europeo

Il Fornitore trasferisce dati fuori dallo Spazio economico europeo solo nei casi dell'Allegato A o su istruzione del Cliente, con le garanzie del Capo V del GDPR.

Assistenza, incidenti e fine del servizio

Art. 9. Richieste degli interessati

9.1 Se riceve una richiesta di un interessato sui dati del Cliente, il Fornitore la inoltra al Cliente senza ritardo e non risponde nel merito.

9.2 Il Cliente risponde agli interessati, usando le funzioni del Software. In modalità Locale il Fornitore non può leggere né estrarre i dati riservati, quindi queste operazioni spettano al Cliente.

Art. 10. Assistenza al Cliente

10.1 Il Fornitore assiste il Cliente, per quanto ragionevole e nei limiti delle informazioni disponibili, per le richieste degli interessati, la sicurezza, le valutazioni d'impatto e i rapporti con il Garante.

10.2 I casi semplici sono inclusi. Sono a pagamento, alla tariffa indicata nel Preventivo o comunicata prima dell'intervento, le attività che richiedono lavoro tecnico o documenti specifici.

Art. 11. Violazioni dei dati

11.1 Il Fornitore avvisa il Cliente entro 48 ore da quando viene a conoscenza di una violazione dei dati trattati per suo conto.

11.2 L'avviso indica, per quanto noto in quel momento, cosa è successo, quali dati riguarda e le misure adottate. Le altre informazioni possono arrivare in più fasi.

11.3 Il Cliente valuta se notificare al Garante e informare gli interessati, e lo fa direttamente. L'avviso del Fornitore non è ammissione di colpa o di responsabilità.

Art. 12. Verifiche

12.1 Il Fornitore mette a disposizione le informazioni necessarie a dimostrare il rispetto dell'art. 28 GDPR, prima di tutto con documenti, report e dichiarazioni scritte.

12.2 Se questi non bastano, il Cliente o un revisore vincolato alla riservatezza, non concorrente del Fornitore, può svolgere una verifica all'anno, con 30 giorni di preavviso scritto e a spese del Cliente. Il tempo del Fornitore è a pagamento.

12.3 La verifica non può riguardare dati di altri clienti, codice sorgente, funzionamento tecnico delle tecnologie del Fornitore o procedure di sicurezza la cui divulgazione ne ridurrebbe l'efficacia. Il preavviso e il limite annuale non si applicano alle richieste di un'autorità competente.

Art. 13. Fine del servizio

13.1 Alla fine del servizio il Cliente può esportare i dati in formato aperto, dal Software o con le modalità dell'Allegato della Formula, per almeno 30 giorni. In modalità Locale l'esportazione si avvia dal terminale del Cliente.

13.2 Trascorso questo periodo, il Fornitore cancella i dati dai sistemi attivi. Dai backup vengono eliminati con il normale ciclo di rotazione, entro 14 giorni, restando protetti e non usati fino ad allora.

13.3 Il Fornitore conserva i dati solo se la legge lo richiede. Su richiesta conferma la cancellazione per iscritto.

Responsabilità e approvazione

Art. 14. Responsabilità

14.1 Tra le parti, anche per questo documento, valgono il limite e le esclusioni dell'art. 21 del Contratto quadro e la manleva dell'art. 22, salvo dolo o colpa grave.

14.2 Questo articolo non limita i diritti degli interessati né i poteri del Garante. Se una parte paga un interessato o subisce una sanzione per una violazione dell'altra, può rivalersi nei limiti dell'art. 82 GDPR e di questo articolo.

14.3 Il Fornitore risponde solo degli obblighi che il GDPR pone a suo carico come responsabile e delle istruzioni lecite del Cliente.

Art. 15. Approvazione specifica (artt. 1341 e 1342 c.c.)

Con il secondo codice OTP previsto dall'art. 27 del Contratto quadro, il Cliente approva specificamente: art. 2.1 (dati sensibili), art. 3.2 e 3.3 (istruzioni), art. 7.3 (unico rimedio), art. 10.2 (assistenza a pagamento), art. 12 (limiti alle verifiche), art. 14 (responsabilità).

Allegato A. Sub-responsabili

Il Fornitore ospita i Software su server propri, in Italia, e non affida ad altri l'ospitalità.

Sub-responsabile	Attività	Dati	Luogo e garanzie
Cloudflare, Inc.	Protezione del traffico da attacchi e bot	Indirizzo IP, tipo di browser, pagina richiesta	Rete globale. EU-U.S. Data Privacy Framework e clausole contrattuali standard
AnyDesk Software GmbH e TeamViewer Germany GmbH, quando usati	Collegamento per il controllo remoto dei terminali durante l'assistenza	Dati di connessione e dispositivo; contenuto dello schermo durante la sessione	Germania

Gli strumenti di intelligenza artificiale dell'art. 15 del Contratto quadro non ricevono dati personali e non sono sub-responsabili.

Allegato B. Misure di sicurezza

Questo allegato descrive cosa fanno le misure. Il loro funzionamento tecnico è riservato.

Area	Misura
Protezione fisica	Server in locale blindato, videosorvegliato, con allarme collegato h24 a vigilanza privata
Protezione dei dati	Cifratura post-quantistica nei limiti dell'applicabilità tecnica, secondo il pacchetto indicato nel Preventivo. Modalità Locale o ACS, come da art. 20.3 del Contratto quadro
Accessi	Accesso del Cliente con email, password e OTP. Accessi di assistenza solo autorizzati, registrati e con report firmato
Rilevamento	Sorveglianza automatica degli eventi di sicurezza sui server e blocco delle minacce, senza lettura del contenuto dei dati del Cliente
Aggiornamenti	Aggiornamenti del Software firmati e registrati
Backup locali	Ogni giorno sul server, con sovrascrittura ogni 5 giorni
Copia fuori sede	Ogni sabato, o comunque entro 7 giorni dalla copia precedente, su supporto fisico cifrato conservato in un luogo diverso dai server. Una copia, sovrascritta a ogni aggiornamento.
Ripristino	Procedura fisica controllata e registrata, con prove periodiche su un campione di sistemi