EDILIZIA IN CLOUD

Accordo per il Trattamento dei Dati Personali

Data Processing Agreement (DPA) — art. 28 GDPR

Costituisce parte integrante e sostanziale dei Termini e Condizioni del Servizio "Edilizia in Cloud". Si applica a tutti i Clienti che utilizzano la Piattaforma a partire dalla Data di Efficacia.

Ultimo aggiornamento: 27 aprile 2026 · **Versione:** 1.0

Premessa operativa. Il presente DPA si intende automaticamente sottoscritto dal Cliente al momento dell'accettazione dei Termini e Condizioni del Servizio. Non è quindi necessaria una sottoscrizione separata, salvo che il Cliente richieda espressamente, per i propri requisiti interni di compliance, la firma di una copia controfirmata. In tal caso, è possibile farne richiesta a info@ediliziaincloud.com.

INDICE

1. Premesse

1.1 Il presente Accordo per il Trattamento dei Dati Personali (il "**DPA**") è stipulato tra:

- **il Cliente**, ovvero la persona giuridica o fisica che ha sottoscritto i Termini e Condizioni del Servizio "Edilizia in Cloud" (di seguito anche il "**Titolare**"); e
- Domus Group S.r.l., con sede in Via Aurelio Saffi 29, 20123 Milano (MI), P.IVA 13132010961 (di seguito "**Edilizia in Cloud**", la "**Società**" o il "**Responsabile**");

(congiuntamente le "**Parti**" e singolarmente la "**Parte**").

1.2 Il presente DPA è stipulato ai sensi dell'art. 28 del Regolamento (UE) 2016/679 ("**GDPR**") e disciplina il trattamento dei Dati Personali eseguito dalla Società per conto del Cliente nell'ambito dell'erogazione del servizio software-as-a-service "Edilizia in Cloud" (il "**Servizio**").

1.3 Il presente DPA **costituisce parte integrante e sostanziale** dei Termini e Condizioni del Servizio. In caso di contrasto tra le previsioni dei Termini e Condizioni e quelle del presente DPA in materia di trattamento di Dati Personali, prevalgono le previsioni del presente DPA.

2. Definizioni

Ai fini del presente DPA, i termini definiti hanno il significato loro attribuito dal GDPR. In particolare:

- **"Dati Personali"**: qualsiasi informazione riguardante una persona fisica identificata o identificabile, che il Cliente carica o gestisce nella Piattaforma in qualità di Titolare, ai sensi dell'art. 4, n. 1) GDPR;
- **"Trattamento"**: qualsiasi operazione o insieme di operazioni eseguite sui Dati Personali, ai sensi dell'art. 4, n. 2) GDPR;
- **"Interessato"**: la persona fisica cui si riferiscono i Dati Personali;
- **"Sub-responsabile"**: il fornitore terzo nominato dalla Società ai sensi dell'art. 28, par. 2 e 4, GDPR;

- **"Violazione di Dati Personali" (o "Data Breach")**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali, ai sensi dell'art. 4, n. 12) GDPR;
- **"Autorità di controllo"**: l'Autorità Garante per la Protezione dei Dati Personali italiana o altra autorità di controllo competente ai sensi del GDPR;
- **"Istruzioni Documentate"**: le istruzioni del Titolare, contenute nel presente DPA, nei Termini e Condizioni del Servizio, nelle configurazioni della Piattaforma operate dal Cliente, e in eventuali ulteriori istruzioni scritte impartite dal Cliente alla Società.

3. Oggetto e durata del DPA

3.1 Il presente DPA disciplina i diritti e gli obblighi delle Parti in relazione al Trattamento dei Dati Personali eseguito dalla Società in qualità di Responsabile per conto del Cliente in qualità di Titolare, in occasione dell'erogazione del Servizio.

3.2 La descrizione del Trattamento (oggetto, durata, natura, finalità, categorie di Interessati e di Dati) è dettagliata nell'Allegato 1.

3.3 Il presente DPA ha efficacia dalla data di accettazione dei Termini e Condizioni del Servizio da parte del Cliente e produce i propri effetti per tutta la durata del rapporto contrattuale, oltre che per il periodo necessario all'espletamento delle operazioni di restituzione e/o cancellazione dei Dati Personali successive alla cessazione del contratto.

4. Ruoli delle Parti

4.1 In relazione ai Dati Personali oggetto del presente DPA:

- il **Cliente** agisce in qualità di **Titolare del trattamento** ai sensi dell'art. 4, n. 7), GDPR;
- la **Società** agisce in qualità di **Responsabile del trattamento** ai sensi dell'art. 4, n. 8), GDPR.

4.2 Resta inteso che, per i Dati Personali relativi alla gestione del rapporto contrattuale tra le Parti (registrazione del Cliente, fatturazione, supporto tecnico, comunicazioni commerciali) e per i dati di navigazione del Sito, la Società agisce in qualità di Titolare autonomo, secondo le modalità descritte nella propria Privacy Policy.

4.3 Nel caso in cui la Società determini autonomamente le finalità e i mezzi del trattamento di taluni Dati Personali (ad esempio per la sicurezza informatica del Servizio o per la generazione di dati aggregati e anonimi), agirà in qualità di Titolare autonomo per detti specifici trattamenti.

5. Obblighi del Titolare (Cliente)

Il Cliente, in qualità di Titolare del trattamento, dichiara e si impegna a:

5.1 Trattare i Dati Personali nel rispetto del GDPR e di ogni altra normativa applicabile in materia di protezione dei dati personali, ivi compresa la specifica normativa di settore (es. art. 4 dello Statuto dei Lavoratori per il monitoraggio dei dipendenti, normativa antiriciclaggio, normativa fiscale).

5.2 Disporre di un'idonea base giuridica (consenso, esecuzione contrattuale, obbligo legale, legittimo interesse, ecc.) per ciascun trattamento eseguito tramite la Piattaforma, ai sensi dell'art. 6 GDPR.

5.3 Fornire agli Interessati l'informativa privacy ai sensi degli artt. 13 e 14 GDPR, nonché raccogliere ogni eventuale consenso necessario.

5.4 In caso di utilizzo di moduli che comportino la geolocalizzazione, il monitoraggio o il controllo a distanza dei propri dipendenti (ad esempio: GPS FleetTrack, timbratura geolocalizzata, controllo dei tempi di lavoro), aver previamente concluso l'**accordo collettivo con le rappresentanze sindacali aziendali** ovvero ottenuto la **previa autorizzazione dell'Ispettorato Nazionale del Lavoro**, ai sensi dell'art. 4 della L. 300/1970 ("Statuto dei Lavoratori"), come modificato dal D.Lgs. 151/2015. Tali adempimenti restano di esclusiva responsabilità del Cliente, il quale tiene la Società indenne da ogni pretesa di terzi connessa alla loro mancata o incompleta esecuzione.

5.5 Configurare correttamente la Piattaforma in modo da rispettare i principi di minimizzazione, esattezza e limitazione della conservazione dei dati (art. 5 GDPR), evitando di caricare dati personali eccedenti, non pertinenti o non più necessari rispetto alle finalità per cui sono stati raccolti.

5.6 **Non caricare nella Piattaforma "categorie particolari di dati"** ai sensi dell'art. 9 GDPR (origine razziale, opinioni politiche, convinzioni religiose, dati genetici, biometrici, sanitari, vita o orientamento sessuale) né dati relativi a condanne penali e reati ai sensi dell'art. 10 GDPR, salvo che ciò sia strettamente necessario all'utilizzo del Servizio (ad

esempio: certificati medici per la gestione delle assenze, dati di idoneità sanitaria al lavoro), nel qual caso il Cliente dovrà disporre di una specifica base giuridica e adottare adeguate misure di protezione aggiuntive.

5.7 Adottare, all'interno della propria organizzazione, adeguate misure di sicurezza tecniche e organizzative complementari a quelle adottate dalla Società (a titolo esemplificativo: gestione corretta delle credenziali di accesso, formazione del personale autorizzato, attivazione dell'autenticazione a due fattori, gestione tempestiva della disabilitazione di account di personale che cessa l'attività).

5.8 Riscontrare direttamente le richieste degli Interessati relative ai Dati Personali trattati nella Piattaforma, avvalendosi del supporto della Società ai sensi dell'art. 11 del presente DPA.

5.9 Notificare prontamente alla Società qualsiasi violazione di Dati Personali di cui venga a conoscenza e che possa coinvolgere l'infrastruttura del Servizio.

5.10 In relazione alle **Funzionalità AI** della Piattaforma, il Titolare è l'unico responsabile dei dati personali che immette nei sistemi AI e dell'uso che fa degli output generati. Il Titolare si impegna a non immettere nelle Funzionalità AI categorie particolari di dati (art. 9 GDPR) o dati relativi a condanne e reati (art. 10 GDPR) salvo che ne ricorrano i presupposti di liceità, e a verificare gli output prima di ogni utilizzo. Il Titolare prende atto che, per l'erogazione delle Funzionalità AI, i dati possono essere trasmessi ai Fornitori AI indicati nell'Allegato 3, in qualità di Sub-responsabili, i quali si sono impegnati a non utilizzare tali dati per l'addestramento dei propri modelli.

6. Obblighi del Responsabile (Edilizia in Cloud)

La Società, in qualità di Responsabile del trattamento, si impegna a:

6.1 Trattare i Dati Personali esclusivamente sulla base delle **Istruzioni Documentate** del Cliente, salvo che il trattamento sia richiesto dal diritto dell'Unione o di uno Stato membro applicabile alla Società. In tale caso, la Società informerà il Cliente di tale obbligo prima del trattamento, salvo che il diritto applicabile lo vieti per importanti motivi di interesse pubblico.

6.2 Trattare i Dati Personali esclusivamente per le finalità di erogazione del Servizio descritte nei Termini e Condizioni e nell'Allegato 1, e **non per finalità ulteriori o diverse**.

6.3 Garantire che le persone autorizzate al trattamento dei Dati Personali nell'ambito della propria organizzazione siano **vincolate al rispetto della riservatezza** mediante apposito impegno contrattuale o vincolo legale di natura analoga, e che ricevano adeguata formazione in materia di protezione dei dati personali.

6.4 Adottare le **misure di sicurezza** tecniche e organizzative descritte all'art. 9 del presente DPA e nell'Allegato 2, in conformità all'art. 32 GDPR.

6.5 Avvalersi di Sub-responsabili soltanto nelle modalità previste dall'art. 7 del presente DPA.

6.6 Tenendo conto della natura del trattamento, **assistere il Cliente** con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare gli obblighi del Cliente di dare seguito alle richieste degli Interessati ai sensi del Capo III del GDPR.

6.7 **Assistere il Cliente** nel garantire il rispetto degli obblighi di cui agli artt. 32-36 GDPR, tenendo conto della natura del trattamento e delle informazioni a sua disposizione.

6.8 Su scelta del Cliente, cancellare o restituire tutti i Dati Personali al termine della prestazione dei servizi, secondo le modalità di cui all'art. 13 del presente DPA.

6.9 Mettere a disposizione del Cliente tutte le informazioni necessarie a dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR e consentire al Cliente di effettuare audit, secondo le modalità di cui all'art. 12 del presente DPA.

6.10 Informare immediatamente il Cliente qualora, a parere della Società, un'istruzione del Titolare violi il GDPR o altre disposizioni in materia di protezione dei dati.

6.11 Tenere un registro delle attività di trattamento svolte per conto del Cliente ai sensi dell'art. 30, par. 2, GDPR.

6.12 Nominare, ove richiesto dalla normativa, un Responsabile della Protezione dei Dati (DPO) ai sensi degli artt. 37-39 GDPR.

7. Sub-responsabili del trattamento

7.1 Il Cliente **autorizza espressamente** la Società ad avvalersi di Sub-responsabili per l'erogazione del Servizio, ai sensi dell'art. 28, par. 2, GDPR. L'elenco dei Sub-responsabili autorizzati al momento dell'accettazione del presente DPA è riportato nell'Allegato 3.

7.2 La Società si impegna a:

- stipulare con ciascun Sub-responsabile un accordo scritto che imponga al Sub-responsabile **obblighi di protezione dei dati di livello equivalente** a quelli previsti dal presente DPA;
- selezionare Sub-responsabili che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate;
- **rispondere pienamente nei confronti del Cliente** dell'inadempimento del Sub-responsabile ai propri obblighi in materia di protezione dei dati.

7.3 La Società si riserva il diritto di modificare l'elenco dei Sub-responsabili in qualsiasi momento, ad esempio per aggiungere nuovi fornitori, sostituire fornitori esistenti o cessare il rapporto con uno di essi. La Società **notificherà** tali modifiche al Cliente con un preavviso di almeno **30 giorni**, mediante:

- aggiornamento della pagina pubblica dei Sub-responsabili (/sub-processors); e/o
- comunicazione email all'indirizzo di contatto del Cliente; e/o
- notifica all'interno della Piattaforma.

7.4 Il Cliente ha facoltà di **opporsi** all'inclusione di un nuovo Sub-responsabile entro 15 giorni dalla notifica, comunicando la propria opposizione, motivata da ragionevoli motivi attinenti alla protezione dei dati, all'indirizzo info@ediliziaincloud.com. In tale caso, le Parti coopereranno in buona fede per individuare una soluzione tecnica alternativa. Qualora non sia possibile individuare una soluzione ragionevole entro 30 giorni, ciascuna Parte avrà facoltà di risolvere il contratto del Servizio (limitatamente alle funzionalità interessate) con effetto immediato.

7.5 La mancata opposizione del Cliente entro il termine di cui al precedente comma comporta l'accettazione tacita del nuovo Sub-responsabile.

7.6 La Società può avvalersi di Sub-responsabili del trattamento **senza preavviso** esclusivamente nei seguenti casi: (i) variazioni della denominazione sociale o trasferimenti di ramo d'azienda di un Sub-responsabile esistente; (ii) sostituzione urgente di un Sub-responsabile per ragioni di sicurezza, continuità del Servizio o altre cause di forza maggiore. In tali casi, la Società ne darà comunicazione al Cliente nel più breve tempo possibile.

8. Trasferimenti extra-UE

8.1 Alcuni Sub-responsabili possono trattare i Dati Personali al di fuori dello **Spazio Economico Europeo** (SEE), tipicamente negli Stati Uniti d'America. Il Cliente ne prende atto e autorizza i trasferimenti per quanto strettamente necessario all'erogazione del Servizio.

8.2 Per ogni trasferimento extra-UE, la Società garantisce la presenza di idonee garanzie ai sensi degli artt. 44-49 GDPR, in particolare:

- **Decisioni di adeguatezza** della Commissione europea (art. 45 GDPR), ove disponibili — ad esempio l'*EU-US Data Privacy Framework* per i fornitori statunitensi che vi abbiano aderito;
- in assenza di decisione di adeguatezza, **Clausole Contrattuali Tipo** approvate dalla Commissione europea con la decisione (UE) 2021/914, eventualmente integrate da misure tecniche e organizzative supplementari (cifratura, pseudonimizzazione, controlli di accesso aggiuntivi);
- in casi residuali, una delle deroghe previste dall'art. 49 GDPR.

8.3 Una copia delle garanzie adottate (estratti delle Clausole Contrattuali Tipo, certificazioni, attestazioni di adesione al Data Privacy Framework) è messa a disposizione del Cliente su richiesta scritta a info@ediliziaincloud.com.

9. Misure di sicurezza tecniche e organizzative

9.1 La Società adotta misure di sicurezza tecniche e organizzative adeguate ai sensi dell'art. 32 GDPR, tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

9.2 Le misure di sicurezza adottate sono dettagliate nell'Allegato 2. Tali misure sono soggette a revisione e aggiornamento periodici per riflettere l'evoluzione tecnologica e dei rischi, fermo restando che la Società non ridurrà unilateralmente il livello complessivo di sicurezza durante la vigenza del presente DPA.

10. Notifica delle violazioni di dati personali

10.1 Qualora la Società venga a conoscenza di una **Violazione di Dati Personali** che riguardi i Dati Personali trattati per conto del Cliente, ne darà notifica al Cliente **senza ingiustificato ritardo** e, ove possibile, **entro 48 ore** dalla scoperta della Violazione.

10.2 La notifica al Cliente conterrà, nella misura in cui le informazioni siano disponibili al momento della notifica:

- la descrizione della natura della Violazione, delle categorie di Interessati e di Dati Personali interessati e del numero approssimativo degli stessi;
- il nome e i dati di contatto del DPO o di altro punto di contatto presso il quale ottenere ulteriori informazioni;
- la descrizione delle probabili conseguenze della Violazione;
- la descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla Violazione e per attenuarne i possibili effetti negativi.

10.3 La Società **collaborerà ragionevolmente** con il Cliente per assisterlo nell'adempimento dei propri obblighi di notifica all'Autorità di controllo (art. 33 GDPR) e di comunicazione agli Interessati (art. 34 GDPR), restando inteso che **tali obblighi di notifica e comunicazione gravano sul Cliente in qualità di Titolare**.

10.4 La notifica al Cliente di una Violazione non costituisce, di per sé, ammissione di responsabilità o colpa da parte della Società.

11. Assistenza al Titolare

11.1 Tenendo conto della natura del trattamento e nella misura in cui ciò sia possibile, la Società assiste il Cliente con misure tecniche e organizzative adeguate per:

- dare seguito alle richieste degli Interessati di esercizio dei diritti di cui agli artt. 15-22 GDPR (accesso, rettifica, cancellazione, limitazione, portabilità, opposizione);
- garantire il rispetto degli obblighi di sicurezza (art. 32 GDPR);
- gestire le notifiche di Violazioni (artt. 33 e 34 GDPR);
- condurre eventuali Valutazioni d'Impatto sulla Protezione dei Dati (DPIA) ai sensi dell'art. 35 GDPR;

- condurre eventuali consultazioni preventive con l'Autorità di controllo ai sensi dell'art. 36 GDPR.

11.2 La Piattaforma mette a disposizione del Cliente **strumenti self-service** (es. esportazione dei dati di un singolo interessato, anonimizzazione, cancellazione) che consentono al Cliente di rispondere autonomamente a gran parte delle richieste degli Interessati. La Società fornirà supporto manuale solo ove tali strumenti non consentano di soddisfare la richiesta.

11.3 Qualora la richiesta del Cliente di assistenza richieda un impegno significativo eccedente l'ordinaria assistenza connessa all'erogazione del Servizio, la Società potrà richiedere il rimborso dei costi ragionevolmente sostenuti, secondo le tariffe orarie comunicate al Cliente prima dell'esecuzione delle attività.

11.4 Qualora la Società riceva direttamente una richiesta di esercizio di diritti da parte di un Interessato, la trasmetterà tempestivamente al Cliente, senza darvi seguito autonomamente, e indicherà all'Interessato di rivolgersi al Cliente.

12. Audit e ispezioni

12.1 La Società mette a disposizione del Cliente, su richiesta scritta, tutte le informazioni ragionevolmente necessarie a dimostrare il rispetto degli obblighi previsti dall'art. 28 GDPR e dal presente DPA. Tali informazioni includono, in via prioritaria:

- copia del presente DPA e degli accordi con i Sub-responsabili (in forma redatta per la riservatezza);
- copia delle eventuali certificazioni di sicurezza ottenute (es. ISO/IEC 27001, SOC 2, ISO/IEC 27701);
- relazioni sintetiche dei test di vulnerabilità, *penetration test* e audit di terze parti, ove disponibili;
- la presente Cookie Policy, Privacy Policy e ogni ulteriore documentazione pubblica relativa al trattamento.

12.2 Qualora le informazioni di cui al precedente comma non siano sufficienti, il Cliente ha diritto di effettuare audit, ispezioni o richieste documentali aggiuntive, alle seguenti condizioni:

- l'audit è condotto a spese del Cliente, salvo che riveli inadempimenti significativi della Società;

- il Cliente fornisce un preavviso scritto di almeno **30 giorni**, salvo nei casi di Violazione di Dati Personali in corso o di indagine dell'Autorità di controllo;
- l'audit non può svolgersi più di **una volta all'anno**, salvo nei casi di cui sopra;
- l'audit è condotto durante l'orario lavorativo, in modo da minimizzare l'impatto sul Servizio, e nel rispetto delle policy di sicurezza e riservatezza della Società;
- il Cliente o il revisore incaricato sono tenuti alla riservatezza di tutte le informazioni acquisite durante l'audit;
- l'audit non può comprendere l'accesso a dati o sistemi di altri clienti della Società.

12.3 In alternativa all'audit diretto, la Società potrà mettere a disposizione del Cliente i risultati di audit indipendenti già condotti da soggetti terzi qualificati (es. revisori, organismi di certificazione), nei limiti consentiti dagli accordi con tali terzi.

13. Restituzione e cancellazione dei dati

13.1 Al termine del rapporto contrattuale, per qualunque causa, la Società consente al Cliente di **esportare i propri Dati Personali** dalla Piattaforma in formati standard (CSV, JSON, XML, PDF) per un periodo di **30 giorni** dalla data di cessazione.

13.2 Decorsi 30 giorni, la Società procederà alla **cancellazione** dei Dati Personali dai sistemi di produzione, fatti salvi:

- i dati che la Società è tenuta a conservare in forza di obblighi di legge (in particolare di natura fiscale, contabile e antiriciclaggio), per il tempo strettamente necessario;
- i dati conservati nei **backup di sicurezza**, che saranno cancellati secondo il normale ciclo di rotazione dei backup, comunque entro un massimo di **90 giorni**;
- i dati strettamente necessari alla difesa di un diritto in giudizio.

13.3 Su richiesta scritta del Cliente, la Società rilascerà un'attestazione formale di avvenuta cancellazione dei Dati Personali.

13.4 In alternativa alla cancellazione, su espressa richiesta del Cliente, la Società può procedere alla **restituzione** dei Dati Personali in formato strutturato e di uso comune. Eventuali servizi professionali di assistenza alla migrazione potranno essere oggetto di tariffazione separata.

14. Responsabilità e indennità

14.1 La responsabilità delle Parti per inadempimento degli obblighi del presente DPA è regolata dagli artt. 82 GDPR e dalla normativa applicabile.

14.2 Ferma restando la responsabilità di ciascuna Parte ai sensi dell'art. 82 GDPR nei confronti degli Interessati, le Parti convengono che **la responsabilità reciproca** derivante dal presente DPA è soggetta alle **limitazioni di responsabilità previste dai Termini e Condizioni del Servizio**, ferma restando la nullità di clausole limitative in caso di dolo o colpa grave o di violazione di norme inderogabili.

14.2-bis Le Parti danno atto che il Cliente, in qualità di Titolare, determina autonomamente finalità e mezzi del trattamento e che la Società, in qualità di Responsabile, agisce esclusivamente sulla base delle istruzioni documentate del Cliente. Conseguentemente, qualora la Società sia tenuta a corrispondere a un Interessato o all'Autorità un risarcimento o una sanzione per una violazione imputabile, in tutto o in parte, alle istruzioni, alle scelte o agli inadempimenti del Cliente, quest'ultimo rimborserà alla Società la quota di responsabilità ad esso ascrivibile ai sensi dell'art. 82, par. 5, GDPR.

14.3 Il Cliente **tiene indenne** la Società da ogni richiesta di risarcimento, sanzione o pretesa proveniente da Interessati, Autorità di controllo o terzi, derivante da:

- violazione, da parte del Cliente, degli obblighi di cui all'art. 5 del presente DPA;
- caricamento nella Piattaforma di Dati Personali eccedenti, non pertinenti, illeciti o privi di idonea base giuridica;
- mancato adempimento, da parte del Cliente, delle proprie obbligazioni di Titolare ai sensi del GDPR (in particolare: informativa, raccolta del consenso, esercizio dei diritti, accordo sindacale ex art. 4 dello Statuto dei Lavoratori).

15. Modifiche al DPA

15.1 La Società si riserva il diritto di aggiornare il presente DPA per riflettere modifiche normative, organizzative o tecniche, nonché per recepire indicazioni delle Autorità di controllo o orientamenti del Comitato Europeo per la Protezione dei Dati (EDPB).

15.2 Le modifiche al DPA saranno comunicate al Cliente con un preavviso di almeno **30 giorni**, mediante email o avviso nella Piattaforma. Le modifiche entrano in vigore alla data indicata nella comunicazione.

15.3 Qualora le modifiche comportino una **riduzione sostanziale** delle tutele riconosciute al Cliente in qualità di Titolare, il Cliente potrà recedere senza costi entro la data di efficacia delle modifiche.

16. Legge applicabile e foro competente

16.1 Il presente DPA è regolato dalla **legge italiana** e dalle disposizioni del GDPR direttamente applicabili.

16.2 Per qualsiasi controversia derivante dal presente DPA o ad esso connessa sarà competente in via esclusiva il **Foro di Milano**, in coerenza con quanto previsto dai Termini e Condizioni del Servizio.

ALLEGATO 1 — DESCRIZIONE DEL TRATTAMENTO

A.1 Oggetto del trattamento

Trattamento dei Dati Personali necessario all'erogazione del Servizio software-as-a-service "Edilizia in Cloud" e alle relative funzionalità sottoscritte dal Cliente.

A.2 Durata del trattamento

Per tutta la durata del contratto del Servizio, oltre al periodo di restituzione/cancellazione di cui all'art. 13 del presente DPA.

A.3 Natura e finalità del trattamento

Il trattamento ha natura automatizzata e include le seguenti operazioni: raccolta, registrazione, organizzazione, strutturazione, conservazione, elaborazione, modifica, estrazione, consultazione, comunicazione mediante trasmissione, raffronto, interconnessione, limitazione, cancellazione e distruzione dei Dati Personali.

Le finalità sono limitate all'erogazione del Servizio, come descritto nei Termini e Condizioni e nei moduli funzionali sottoscritti dal Cliente.

A.4 Categorie di Interessati

I Dati Personali trattati possono riferirsi alle seguenti categorie di Interessati, in funzione delle scelte operative del Cliente:

- **Dipendenti, collaboratori e operai** del Cliente, inclusi addetti di cantiere e personale tecnico/amministrativo;
- **Utenti autorizzati** del Cliente alla Piattaforma (referenti, amministratori, capi cantiere);
- **Clienti finali** del Cliente (committenti, condomini, privati e imprese che ricevono prestazioni edili dal Cliente);
- **Fornitori, subappaltatori, professionisti** con cui il Cliente intrattiene rapporti commerciali;

- **Visitatori e contatti commerciali** registrati dal Cliente nella Piattaforma a fini di gestione di lead, preventivi e CRM.

A.5 Categorie di Dati Personali

Categoria	Tipologia di dati (esemplificativa)
Dati identificativi e di contatto	Nome, cognome, ragione sociale, codice fiscale, P.IVA, indirizzo, telefono, email, PEC
Dati relativi al rapporto di lavoro	Mansione, livello, retribuzione, contratto applicato, presenze, ferie, permessi, malattia, cedolini, comunicazioni obbligatorie
Dati di geolocalizzazione	Posizione GPS dei mezzi e degli operatori, timbrature geolocalizzate (in caso di attivazione dei moduli FleetTrack e timbratura)
Dati di sicurezza sul lavoro	DPI assegnati, formazione svolta, idoneità sanitarie, sopralluoghi, incidenti
Dati contabili e di pagamento	Fatture, scadenzari, IBAN, dati di pagamento, dati bancari (PSD2)
Dati di cantiere e operativi	Lavori, preventivi, contratti d'appalto, DDT, materiali, mezzi, comunicazioni
Dati documentali	Documenti, file, comunicazioni, ticket, allegati caricati nella Piattaforma
Dati biometrici tecnici	In caso di utilizzo della firma elettronica avanzata (FEA), parametri tecnici della firma grafometrica
Categorie particolari (art. 9 GDPR)	Solo se caricati dal Cliente: certificati medici, idoneità sanitarie, documenti relativi a salute e sicurezza dei lavoratori

ALLEGATO 2 — MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE (TOM)

B.1 Sicurezza dei dati in transito

- Cifratura di tutte le comunicazioni client-server mediante protocollo **TLS 1.2 o superiore**;
- Disabilitazione di protocolli e cifrari obsoleti;
- Certificati TLS gestiti tramite Certificate Authority pubbliche con rinnovo automatico;
- HSTS (HTTP Strict Transport Security) attivo su tutti i domini.

B.2 Sicurezza dei dati a riposo

- Cifratura at-rest dei database e degli storage applicativi mediante algoritmi standard di settore (**AES-256**);
- Cifratura at-rest dei backup;
- Gestione delle chiavi di cifratura tramite key management service del provider cloud, con rotazione periodica.

B.3 Controllo degli accessi

- Autenticazione delle utenze applicative mediante credenziali personali univoche;
- Politiche di password forti (lunghezza minima, complessità, blocco dopo tentativi falliti);
- Supporto all'autenticazione a più fattori (2FA) per gli utenti applicativi;
- Controllo degli accessi basato sui ruoli (**RBAC**) con principio del minimo privilegio;
- **Row-Level Security** a livello di database multi-tenant, che garantisce la segregazione logica dei dati di ciascun Cliente;
- Accessi amministrativi all'infrastruttura limitati a personale autorizzato, registrati e periodicamente rivisti.

B.4 Sicurezza infrastrutturale

- Hosting su infrastrutture cloud di provider qualificati (vedi Allegato 3) con punti di presenza nello Spazio Economico Europeo;
- Protezione perimetrale tramite Web Application Firewall (Cloudflare);

- Protezione DDoS e bot management;
- Segregazione di rete tra ambienti di produzione, staging e sviluppo;
- Segreti applicativi (API key, credenziali) gestiti tramite vault dedicati e mai inseriti nel codice sorgente.

B.5 Backup e continuità operativa

- Backup automatici giornalieri dei database con politica di rotazione e ridondanza geografica;
- Test periodici delle procedure di ripristino;
- RPO (Recovery Point Objective) target: **24 ore**;
- RTO (Recovery Time Objective) target: **8 ore** per gli incidenti maggiori.

B.6 Gestione degli incidenti e dei data breach

- Procedure documentate di gestione degli incidenti di sicurezza;
- Monitoraggio continuo dei sistemi e degli accessi anomali;
- Conservazione dei log applicativi e di accesso per il tempo necessario alle finalità di sicurezza;
- Procedura di notifica al Cliente entro 48 ore in caso di Violazione di Dati Personali (art. 10 del DPA).

B.7 Misure organizzative

- Personale autorizzato al trattamento, formato e vincolato al segreto professionale;
- Code review obbligatoria per le modifiche al codice di produzione;
- Test automatici di sicurezza nel ciclo di sviluppo del software;
- *Penetration test* periodici condotti da soggetti qualificati;
- Aggiornamenti di sicurezza tempestivi delle dipendenze applicative;
- Politiche interne di gestione dei dispositivi (BYOD, MDM) e delle credenziali.

B.8 Privacy by design e by default

- Minimizzazione dei dati raccolti dalla Piattaforma in funzione delle finalità del Servizio;
- Configurazioni di privacy di default impostate sul livello di protezione più elevato compatibile con la funzionalità;
- Funzionalità self-service per l'esercizio dei diritti degli Interessati e per la cancellazione dei dati;
- Documentazione interna dei trattamenti effettuati per conto dei Clienti.

ALLEGATO 3 — SUB-RESPONSABILI AUTORIZZATI

L'elenco aggiornato dei Sub-responsabili è disponibile sulla pagina /sub-processors e viene mantenuto in tempo reale. Il presente Allegato riporta lo stato dei Sub-responsabili alla data di pubblicazione del DPA.

Sub-responsabile	Servizio fornito	Ubicazione	Garanzia trasferimento
Supabase Inc.	Database, autenticazione, storage applicativo	UE (Francoforte)	SCC + DPA
Cloudflare Inc.	CDN, Web Application Firewall, hosting frontend (Pages)	UE / USA	DPF + SCC
Stripe Payments Europe Ltd.	Gestione pagamenti carte e abbonamenti	UE (Irlanda) / USA	DPF + SCC
GoCardless Ltd.	Iniziazione pagamenti e Account Information PSD2	UE / Regno Unito	Decisione di adeguatezza UK
Aruba S.p.A.	Trasmissione e ricezione fatture elettroniche SDI, conservazione digitale a norma	Italia / UE	Trattamento UE
Telnyx LLC	SMS transazionali e marketing, infrastruttura voce	UE / USA	SCC
ElevenLabs Inc.	Sintesi vocale per agenti vocali AI	USA	SCC
Meta Platforms Ireland Ltd.	WhatsApp Business / Cloud API	UE (Irlanda) / USA	DPF + SCC
OpenRouter, Inc.	Aggregatore di modelli AI (instradamento richieste LLM)	USA	SCC
Anthropic PBC	Modelli di linguaggio AI (Claude)	USA	SCC + zero data retention API
OpenAI Ireland Ltd. / OpenAI L.L.C.	Modelli di linguaggio e generazione immagini (GPT, GPT-image, DALL·E)	UE (Irlanda) / USA	DPF + SCC + zero data retention API
Moonshot AI	Modelli di linguaggio AI (Kimi), via OpenRouter	Extra-UE	SCC
Google Ireland Ltd. / Google LLC	Modelli AI Gemini, Google Maps, sync Calendar, Analytics 4	UE / USA	DPF + SCC
Altri Fornitori AI via OpenRouter (DeepSeek, xAI, Meta, Mistral, Cohere, Qwen, Perplexity e ulteriori)	Modelli di linguaggio, ricerca semantica ed embeddings	UE / USA / Extra-UE	SCC
Replicate, Inc.	Generazione di immagini e video (incl. MiniMax)	USA	SCC

Sub-responsabile	Servizio fornito	Ubicazione	Garanzia trasferimento
Twilio Inc. — SendGrid	Email transazionali	USA	DPF + SCC
Resend, Inc.	Email transazionali	USA	SCC
Elastic Email Inc.	Email di marketing	UE / USA	SCC
Apple Inc.	Sincronizzazione calendario Apple (CalDAV)	USA	SCC
[provider FEA da definire]	Firma Elettronica Avanzata	UE	Trattamento UE

Legenda: SCC = Standard Contractual Clauses (Clausole Contrattuali Tipo della Commissione UE); DPF = EU-US Data Privacy Framework; DPA = Data Processing Agreement con il sub-responsabile.

Sottoscrizione (opzionale)

Il presente DPA si intende validamente accettato dal Cliente con l'accettazione dei Termini e Condizioni del Servizio. La sottoscrizione del presente blocco è prevista esclusivamente per i Clienti che, in conformità ai propri requisiti interni di compliance, richiedano una copia controfirmata del documento.

Per il Titolare (Cliente)

Ragione sociale:

_____

Sede legale:

_____

P.IVA: _____

Rappresentante legale:

_____

_____

Firma e timbro · Data: ____ / ____ / ____

Per il Responsabile (Edilizia in Cloud)

Domus Group S.r.l.

Sede legale: Via Aurelio Saffi 29, 20123 Milano (MI)

P.IVA: 13132010961

Rappresentante legale: 13132010961

_____

Firma e timbro · Data: ____ / ____ / ____