iWebLab S.r.l.
Strada Nona Guladaria 68 — 47895 Domagnano — Repubblica di San Marino — COE SM30107

Accordo sul trattamento dei dati personali

Data Processing Agreement — art. 28 Regolamento (UE) 2016/679 — versione 1.0

Campo	Valore
Versione	1.0
In vigore dal	6 ottobre 2026
Emesso da	iWebLab S.r.l.
Ambito	Tutti i servizi erogati da iWebLab S.r.l. che comportino trattamento di dati personali per conto del Cliente
Testo vigente	https://iweblab.it/docs/dpa/
Elenco sub-responsabili	https://iweblab.it/docs/sub-responsabili/
Allegati	A — Servizi, dati e interessati · B — Misure di sicurezza · C — Sub-responsabili · D — Valutazione d'impatto sul trasferimento · Appendice SCC

Il presente accordo costituisce parte integrante delle Condizioni Generali di Contratto di iWebLab S.r.l. e si applica automaticamente a ogni rapporto che comporti trattamento di dati personali per conto del Cliente, senza necessità di sottoscrizione separata. Su richiesta del Cliente, iWebLab emette copia sottoscritta di contenuto identico.

Art. 1 — Definizioni Ai fini del presente accordo:

- "GDPR" indica il Regolamento (UE) 2016/679;
- "Cliente" indica il soggetto che ha stipulato con iWebLab il contratto di servizio;
- "iWebLab" indica iWebLab S.r.l., con sede in Strada Nona Guladaria 68, 47895 Domagnano, Repubblica di San Marino, COE SM30107;
- "Servizi" indica le prestazioni oggetto del contratto, come specificate in Allegato A;
- "Dati" indica i dati personali trattati da iWebLab per conto del Cliente nell'ambito dei Servizi;
- "SCC" indica le Clausole Contrattuali Tipo adottate con Decisione di esecuzione (UE) 2021/914.

I termini non altrimenti definiti hanno il significato loro attribuito dall'art. 4 GDPR. Gli Allegati costituiscono parte integrante e sostanziale del presente accordo.

Art. 2 — Ambito e qualificazione delle Parti

2.1 Cliente Titolare

Ove il Cliente determini autonomamente finalità e mezzi del trattamento, esso agisce quale Titolare e iWebLab quale Responsabile ai sensi dell'art. 28 GDPR.

2.2 Cliente Responsabile (agenzie, rivenditori, fornitori di servizi)

Ove il Cliente tratti i Dati per conto di propri clienti, agendo quindi quale Responsabile, iWebLab agisce quale sub-responsabile. In tal caso:

- il Cliente dichiara di aver ottenuto dal rispettivo titolare l'autorizzazione a ricorrere a sub-responsabili, generale o specifica, e di essere legittimato a impartire le istruzioni di cui al presente accordo;
- le obbligazioni qui poste a carico di iWebLab si intendono assunte a beneficio del titolare per il cui conto il Cliente opera;
- ogni riferimento al "Titolare" contenuto nel presente accordo si intende riferito al Cliente nella sua qualità di Responsabile, salvo quanto necessariamente riferibile al titolare originario.

La qualificazione di cui al presente paragrafo si applica ove il Cliente abbia dichiarato, in fase d'ordine o nell'area riservata, di trattare i Dati per conto di terzi. In difetto di tale dichiarazione, il Cliente è considerato Titolare ai sensi del paragrafo 2.1. La dichiarazione è registrata con data e ora e determina il modulo delle SCC applicabile ai sensi dell'art. 11.2.

2.3 Trattamenti in cui iWebLab agisce quale Titolare autonomo

iWebLab agisce quale titolare autonomo, al di fuori del presente accordo, in relazione ai dati di gestione del rapporto contrattuale con il Cliente: anagrafica, dati di fatturazione, corrispondenza commerciale, richieste di assistenza, log di accesso alle aree riservate. Tali trattamenti sono disciplinati dall'informativa resa ai sensi degli artt. 13 e 14 GDPR.

Art. 3 — Oggetto, natura e durata iWebLab tratta i Dati esclusivamente per l'erogazione dei Servizi effettivamente attivati dal Cliente. Oggetto, natura, finalità, categorie di dati e categorie di interessati sono specificati in Allegato A. Il trattamento ha durata pari a quella del rapporto contrattuale relativo a ciascun Servizio e cessa con esso, fatto salvo quanto previsto all'art. 12.

Le Parti danno atto che, per i rapporti già in corso alla data di entrata in vigore del presente accordo, il trattamento è in essere sin dall'attivazione dei Servizi ed è stato svolto in conformità ai principi qui formalizzati; il presente atto ha pertanto anche funzione ricognitiva.

Art. 4 — Istruzioni documentate iWebLab tratta i Dati soltanto su istruzione documentata del Cliente. Costituiscono istruzioni documentate il contratto di servizio, il presente accordo e i relativi allegati, la documentazione tecnica dei Servizi, nonché le richieste inoltrate dal Cliente tramite i canali di assistenza ufficiali. Le Parti riconoscono espressamente che rientrano fra le istruzioni documentate, in quanto necessarie all'erogazione e alla sicurezza dei Servizi:

- la conservazione e l'analisi automatizzata dei log tecnici del server web (access log ed error log) per finalità di rilevamento di intrusioni, attività malevole e anomalie di sicurezza, secondo le modalità e le garanzie di cui all'Allegato B, sezione 6;
- l'esecuzione, la conservazione, la verifica e il ripristino delle copie di sicurezza;
- il filtraggio dei messaggi di posta elettronica a fini antispam e antivirus, ove il relativo Servizio sia attivo;
- gli interventi tecnici di manutenzione, aggiornamento, mitigazione di attacchi e ripristino della continuità operativa, ivi compresa la sospensione temporanea di risorse compromesse;
- la trasmissione dei dati di registrazione ai registri dei nomi a dominio, ove il relativo Servizio sia attivo.

iWebLab informa immediatamente il Cliente qualora ritenga che un'istruzione violi il GDPR o altre disposizioni applicabili in materia di protezione dei dati, e può sospenderne l'esecuzione fino a conferma scritta.

Art. 5 — Riservatezza e persone autorizzate iWebLab garantisce che l'accesso ai Dati sia limitato al personale la cui attività lo renda necessario e che tale personale si sia impegnato per iscritto alla riservatezza, con vincolo che permane oltre la cessazione del rapporto, ai sensi dell'art. 28, par. 3, lett. b)

GDPR. L'accesso amministrativo all'infrastruttura è consentito esclusivamente a personale nominativamente individuato, secondo quanto descritto in Allegato B, sezione 3.

Art. 6 — Misure di sicurezza iWebLab adotta le misure tecniche e organizzative descritte in Allegato B, adeguate al rischio ai sensi dell'art. 32 GDPR, tenuto conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento. iWebLab può modificare le misure in ragione dell'evoluzione tecnologica o delle minacce, purché il livello di sicurezza complessivo non risulti diminuito. Le modifiche sostanziali sono comunicate secondo le modalità di cui all'art. 15. Il Cliente riconosce che il livello di sicurezza complessivo dipende anche dalla corretta gestione applicativa di propria competenza, come specificato in Allegato B, sezione 8.

Art. 7 — Sub-responsabili Il Cliente autorizza in via generale, ai sensi dell'art. 28, par. 2, GDPR, il ricorso da parte di iWebLab a sub-responsabili per l'erogazione dei Servizi. L'elenco aggiornato dei sub-responsabili è pubblicato all'indirizzo indicato in copertina e riprodotto, alla data di emissione del presente accordo, in Allegato C. Il Cliente può iscriversi al servizio di notifica degli aggiornamenti. iWebLab comunica al Cliente, con preavviso di almeno 30 giorni, l'intenzione di aggiungere o sostituire un sub-responsabile. Entro tale termine il Cliente può opporsi per motivi ragionevoli e documentati connessi alla protezione dei dati. In difetto di accordo entro i successivi 30 giorni, il Cliente può recedere dai Servizi interessati senza penali e con rimborso pro rata dei corrispettivi versati e non goduti. iWebLab impone contrattualmente a ciascun sub-responsabile obblighi di protezione dei dati non meno onerosi di quelli previsti dal presente accordo e risponde del loro operato come del proprio. Non costituiscono sub-responsabili i fornitori che non compiono operazioni su dati personali per conto di iWebLab, quali i fornitori di housing indicati in Allegato C, sezione 2.

Art. 8 — Diritti degli interessati Tenuto conto della natura del trattamento, iWebLab assiste il Cliente con misure tecniche e organizzative adeguate al fine di dare seguito alle richieste di esercizio dei diritti di cui al Capo III GDPR, nella misura in cui il Cliente non possa provvedervi autonomamente mediante gli strumenti di amministrazione messi a disposizione. iWebLab che riceva direttamente una richiesta da un interessato si astiene dal rispondere nel merito e la trasmette al Cliente senza ingiustificato ritardo. Il Cliente prende atto che i Dati oggetto di richiesta di cancellazione permangono nelle copie di sicurezza fino alla naturale rotazione delle stesse, secondo i termini di cui all'art. 12.

Art. 9 — Assistenza al Cliente iWebLab assiste il Cliente nel garantire il rispetto degli obblighi di cui agli artt. da 32 a 36 GDPR, tenuto conto della natura del trattamento e delle informazioni a sua disposizione, mettendo a disposizione la documentazione tecnica pertinente, ivi compresi gli allegati al presente accordo, utilizzabili quale base per la valutazione d'impatto di cui all'art. 35 GDPR.

Art. 10 — Violazioni di dati personali iWebLab notifica al Cliente ogni violazione di dati personali che coinvolga i Dati senza ingiustificato ritardo e comunque entro 48 ore dal momento in cui ne ha acquisito conoscenza, all'indirizzo di posta elettronica indicato dal Cliente nell'area riservata. La notifica descrive, nella misura in cui le informazioni siano disponibili: la natura della violazione; le categorie e il numero approssimativo di interessati e di record coinvolti; le probabili conseguenze; le misure adottate o proposte per porvi rimedio e attenuarne gli effetti; un recapito per ulteriori informazioni. Ove non sia possibile fornire le informazioni contestualmente, esse sono trasmesse in fasi successive senza ulteriore ingiustificato ritardo. iWebLab documenta le violazioni e coopera con il Cliente per consentirgli l'adempimento dei propri obblighi.

Restano di competenza esclusiva del Cliente la valutazione circa la notifica all'Autorità di controllo ai sensi dell'art. 33 GDPR e l'eventuale comunicazione agli interessati ai sensi dell'art. 34 GDPR.

Art. 11 — Trasferimenti verso paesi terzi

11.1 Ubicazione dei dati

I Dati in produzione sono ospitati su infrastruttura ubicata nello Spazio Economico Europeo, secondo quanto specificato in Allegato B, sezione 1. Le copie di sicurezza sono conservate nello Spazio Economico Europeo.

11.2 Accesso da parte di iWebLab

iWebLab è stabilita nella Repubblica di San Marino, Stato non destinatario, alla data di emissione del presente accordo, di decisione di adeguatezza ai sensi dell'art. 45 GDPR. L'accesso ai Dati da parte del personale di iWebLab costituisce pertanto trasferimento verso paese terzo ai sensi del Capo V GDPR, ancorché i server siano ubicati nello Spazio Economico Europeo. Tale trasferimento è assistito dalle garanzie adeguate di cui all'art. 46, par. 2, lett. c) GDPR mediante le SCC, che si intendono integralmente richiamate e incorporate nel presente accordo. Si applica il Modulo 2 (titolare-responsabile); si applica il Modulo 3 (responsabile-sub-responsabile) ove il Cliente abbia reso la dichiarazione di cui all'art. 2.2. Le opzioni delle clausole 7, 9, 11, 13, 17 e 18 sono esercitate come indicato in Appendice, che riporta altresì la compilazione degli Allegati I e II. L'accettazione del presente accordo da parte del Cliente vale quale adesione alle SCC. Su richiesta, iWebLab emette copia sottoscritta delle SCC. La valutazione d'impatto sul trasferimento richiesta dalla clausola 14 delle SCC è riportata in Allegato D.

11.3 Prevalenza

In caso di contrasto fra le disposizioni del presente accordo e quelle delle SCC, prevalgono queste ultime.

11.4 Servizio di distribuzione dei contenuti e risoluzione DNS

Il servizio di distribuzione dei contenuti (CDN), ove attivo, si avvale di punti di presenza ubicati nello Spazio Economico Europeo e negli Stati Uniti d'America. Il servizio di risoluzione DNS autorevole per i nomi a dominio del Cliente si avvale di nodi ubicati nello Spazio Economico Europeo e negli Stati Uniti d'America. I fornitori e le ubicazioni sono indicati in Allegato C.

In conseguenza di tale architettura, dati personali riferibili ai visitatori dei siti del Cliente — fra cui l'indirizzo IP, ovvero una porzione di esso, e i dati tecnici di connessione — sono trattati anche presso i nodi ubicati negli Stati Uniti d'America.

L'attivazione del servizio da parte del Cliente costituisce istruzione documentata ai sensi dell'art. 28, par. 3, lett. a), del Regolamento. Il trasferimento è assistito dalle garanzie di cui al Capo V del Regolamento indicate in Allegato C e valutate in Allegato D, sezione D.9.

Il Cliente che non intenda avvalersi di nodi ubicati in Paesi terzi può richiedere in ogni momento la disattivazione del servizio di distribuzione dei contenuti, restando i propri siti raggiungibili direttamente sull'infrastruttura di origine, ubicata nello Spazio Economico Europeo. La risoluzione DNS autorevole è invece necessaria al funzionamento dei nomi a dominio e non è disattivabile singolarmente; il Cliente può delegare i propri nomi a dominio a nameserver di terzi.

Ogni variazione delle ubicazioni è comunicata al Cliente ai sensi dell'art. 15.

11.5 Ulteriori trasferimenti

iWebLab non effettua ulteriori trasferimenti al di fuori dello Spazio Economico Europeo senza previa informativa al Cliente e senza aver predisposto adeguate garanzie ai sensi del Capo V GDPR.

Art. 12 — Restituzione e cancellazione Alla cessazione del rapporto, a scelta del Cliente, iWebLab restituisce i Dati o li cancella. Il Cliente può richiedere l'esportazione dei Dati entro 30 giorni dalla cessazione, avvalendosi degli strumenti messi a disposizione ovvero richiedendo assistenza. Decorso tale termine, i Dati sono cancellati dai sistemi di produzione. I Dati permangono nelle copie di sicurezza fino alla naturale rotazione delle stesse, secondo i termini di conservazione indicati in Allegato B, sezione 5 e nella scheda tecnica del piano attivo; decorso tale periodo la cancellazione è definitiva e irreversibile. Restano salvi gli obblighi di conservazione previsti dalla normativa applicabile a iWebLab.

Art. 13 — Verifiche e audit iWebLab mette a disposizione del Cliente la documentazione necessaria a dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR, ivi compresi gli allegati al presente accordo e le eventuali certificazioni possedute o attestazioni dei propri fornitori. Ove tale documentazione non sia sufficiente, il Cliente può svolgere attività di verifica presso iWebLab, con preavviso scritto di almeno 30

giorni, non più di una volta per anno solare, salvo il caso di violazione di dati personali accertata o di specifica richiesta di un'Autorità di controllo. Le verifiche si svolgono in orario lavorativo, senza pregiudizio per la continuità del servizio, e non possono comportare l'accesso a dati di altri clienti di iWebLab, a informazioni coperte da segreto industriale o a elementi la cui divulgazione pregiudicherebbe la sicurezza dell'infrastruttura. Il personale incaricato della verifica è vincolato a obblighi di riservatezza. Gli oneri della verifica sono a carico del Cliente, salvo che essa accerti un inadempimento sostanziale di iWebLab.

Art. 14 — Obblighi del Cliente e responsabilità Il Cliente garantisce la liceità dei Dati conferiti e delle istruzioni impartite, di aver reso agli interessati le informative dovute e di disporre di una base giuridica idonea per i trattamenti affidati a iWebLab. Il Cliente non è autorizzato a trattare per il tramite dei Servizi categorie particolari di dati ai sensi degli artt. 9 e 10 GDPR in assenza di preventivo accordo scritto con iWebLab, volto a definire le misure aggiuntive eventualmente necessarie. Il Cliente prende atto che i contenuti caricati sui Servizi sono determinati esclusivamente da esso e che iWebLab non li seleziona, non li controlla e non ne ha conoscenza preventiva. Ciascuna Parte risponde dei danni cagionati dal trattamento in conformità all'art. 82 GDPR. Le limitazioni di responsabilità previste dal contratto di servizio si applicano al presente accordo nei limiti consentiti dalla normativa applicabile e non operano rispetto ai diritti degli interessati.

Art. 15 — Modifiche e versionamento iWebLab può aggiornare il presente accordo per adeguarlo a modifiche normative, all'evoluzione dei Servizi o a determinazioni delle Autorità competenti. Le modifiche sostanziali sono comunicate al Cliente con preavviso di almeno 30 giorni, mediante posta elettronica all'indirizzo indicato nell'area riservata e pubblicazione all'indirizzo indicato in copertina. Entro tale termine il Cliente può recedere dai Servizi interessati senza penali; la prosecuzione del rapporto vale quale accettazione.

Tutte le versioni sono conservate e restano accessibili a indirizzo permanente. Ciascuna versione è identificata da numero, data di entrata in vigore e impronta crittografica del documento.

Art. 16 — Accettazione e prova Il presente accordo è accettato dal Cliente contestualmente alle Condizioni Generali di Contratto, in forma elettronica ai sensi dell'art. 28, par. 9, GDPR. iWebLab registra e conserva, quale prova dell'accettazione: identificativo del Cliente, data e ora, indirizzo IP di provenienza e impronta crittografica della versione accettata.

Art. 17 — Legge applicabile e foro competente In deroga a quanto previsto dalle Condizioni Generali di Contratto, e limitatamente al presente accordo e alle SCC in esso incorporate, si applica la legge italiana, che ammette i diritti dei terzi beneficiari ai sensi dell'art. 1411 del codice civile. Per ogni controversia derivante dal presente accordo è competente in via esclusiva il Foro di Rimini. Per le controversie derivanti dalle SCC sono competenti i giudici della Repubblica Italiana, e fra essi il Foro di Rimini, fermo il diritto degli interessati di promuovere azione dinanzi al giudice dello Stato membro in cui hanno la residenza abituale, ai sensi della clausola 18, lettera c), delle SCC. La clausola di foro esclusivo rientra fra quelle soggette ad approvazione specifica ai sensi degli artt. 1341 e 1342 del codice civile e va inclusa nell'elenco delle clausole approvate con la seconda spunta in fase d'ordine.

iWebLab S.r.l. — Il legale rappresentante Giuseppe Semeraro

_____

Allegato A — Servizi, categorie di dati e di interessati

Il presente allegato descrive la totalità dei Servizi erogati da iWebLab. Si applicano al singolo Cliente esclusivamente le voci relative ai Servizi effettivamente attivati, come risultanti dal contratto e dall'area riservata.

A.1 Servizi e trattamenti

Servizio	Operazioni di trattamento	Categorie di dati trattate
Hosting gestito	Conservazione, elaborazione, trasmissione, duplicazione a fini di continuità, cancellazione	Contenuti applicativi e database del Cliente; metadati tecnici di traffico
Posta elettronica	Conservazione, trasmissione, filtraggio antispam e antivirus, duplicazione, cancellazione	Metadati e contenuti dei messaggi; dati identificativi dei corrispondenti
Backup	Duplicazione, cifratura, conservazione, ripristino, cancellazione	Copia dei dati ospitati
DNS autoritativo	Conservazione e pubblicazione dei record di zona	Dati tecnici di zona; indirizzi IP dei richiedenti
CDN / edge caching	Elaborazione delle richieste, conservazione temporanea in cache, registrazione dei log	Metadati di richiesta; copia dei contenuti pubblicati
Registrazione domini	Trasmissione ai registri, conservazione, aggiornamento	Dati di registrazione del titolare del dominio e dei contatti
Analisi di sicurezza	Elaborazione automatizzata dei log tecnici	Metadati tecnici di traffico (access log ed error log)

A.2 Finalità

Erogazione dei Servizi contrattualmente convenuti e garanzia della loro sicurezza, integrità, disponibilità e continuità operativa. È esclusa ogni finalità ulteriore, in particolare commerciale, di profilazione o di analisi comportamentale degli interessati.

A.3 Categorie di dati personali

Le categorie di dati sono determinate esclusivamente dal Cliente, che ne dispone il caricamento sui Servizi. iWebLab non seleziona né controlla i contenuti. In via tipica:

Categoria Esemplificazione
Dati identificativi e di contatto Nome, cognome, indirizzo di posta elettronica, telefono, indirizzo, presenti in
database applicativi, moduli web e caselle di posta
Contenuti di comunicazioni Corpo e allegati dei messaggi di posta elettronica ospitati
Dati di clienti e utenti del Cliente Anagrafiche, ordini, transazioni, contenuti generati dagli utenti presenti nelle
applicazioni ospitate
Metadati tecnici di traffico Indirizzi IP, user agent, referer, URL richiesti, codici di risposta, timestamp
Credenziali applicative Chiavi di accesso a webservice trasmesse dalle applicazioni del Cliente; cfr.
Categoria Esemplificazione

Allegato B, sezione 6

Dati di registrazione dei domini Dati del titolare del nome a dominio e dei contatti amministrativo e tecnico

Il trattamento di categorie particolari di dati ai sensi degli artt. 9 e 10 GDPR è soggetto a quanto previsto dall'art. 14 dell'accordo.

A.4 Categorie di interessati

- clienti e utenti finali del Cliente;
- contatti commerciali e potenziali clienti del Cliente;
- dipendenti, collaboratori e fornitori del Cliente;
- visitatori dei siti web e destinatari delle comunicazioni gestite tramite i Servizi;
- ove il Cliente agisca quale Responsabile, gli interessati dei titolari per il cui conto opera.

A.5 Frequenza e durata

Il trattamento è continuativo per l'intera durata del rapporto contrattuale relativo a ciascun Servizio.

Allegato B — Misure tecniche e organizzative

Misure adottate ai sensi dell'art. 32 GDPR e della clausola 8.6 delle SCC.

B.1 Ubicazione e sicurezza fisica

- Infrastruttura di produzione ospitata presso datacenter ubicato in Torino, Italia, in regime di housing: il fornitore eroga esclusivamente spazio rack, alimentazione elettrica e connettività.
- Armadio rack dedicato, chiuso a chiave, con accesso riservato a personale nominativamente individuato di iWebLab.
- Apparati server, storage e di rete di proprietà di iWebLab; il fornitore di housing non dispone di credenziali amministrative né di accesso logico ai sistemi.
- Controllo degli accessi fisici, registrazione degli ingressi e videosorveglianza a cura della struttura ospitante.
- Alimentazione ridondata con gruppi di continuità e generazione di emergenza; connettività ridondata; controllo ambientale a cura della struttura ospitante.

B.2 Segmentazione e architettura di rete

- Nessun sistema di gestione dell'infrastruttura (nodi di virtualizzazione, storage, apparati di rete) è esposto su rete pubblica.
- Reti di gestione, di storage e di produzione segmentate su VLAN e interfacce fisiche dedicate.
- Le macchine virtuali dei clienti sono isolate su VLAN dedicate ed espongono la sola rete pubblica necessaria all'erogazione del Servizio.
- Firewall perimetrale con regole di filtraggio e segregazione fra segmenti.

B.3 Controllo degli accessi amministrativi

- Accesso amministrativo esclusivamente tramite tunnel cifrati WireGuard permanenti fra le sedi di iWebLab, con materiale crittografico custodito sugli apparati firewall e non estraibile dalle postazioni.
- Accesso consentito esclusivamente a personale nominativamente individuato, da postazioni autorizzate; alla data di emissione, un incaricato e una postazione autorizzata.

- Credenziali personali e distinte per ciascun incaricato sui sistemi di virtualizzazione e sui server, con attribuzione univoca delle operazioni. L'attivazione di ulteriori utenze comporta l'assegnazione di credenziali nominative distinte.
- Autenticazione a due fattori (TOTP) sull'interfaccia di gestione della piattaforma di virtualizzazione.
- Accesso SSH ai nodi mediante autenticazione a chiave, con autenticazione tramite password disabilitata.
- Registrazione degli accessi amministrativi e conservazione dei relativi log.
- Procedura di revoca delle abilitazioni alla cessazione del rapporto o in caso di smarrimento di un dispositivo autorizzato.
- Procedura di accesso di emergenza documentata, con credenziali di ripristino conservate fuori banda in luogo protetto, per garantire la continuità della gestione in caso di indisponibilità dell'incaricato.
- Impegno scritto alla riservatezza sottoscritto da ciascun incaricato ai sensi dell'art. 28, par. 3, lett. b) GDPR.

B.4 Cifratura e protezione dei supporti

- Cifratura in transito: TLS sui servizi pubblici (web, posta, pannelli di controllo) con configurazione conforme alle raccomandazioni correnti; tunnel WireGuard sui collegamenti fra sedi.
- Cifratura della copia di sicurezza off-site.
- I Dati in produzione risiedono su cluster di storage distribuito che frammenta gli oggetti su più supporti e più nodi: il singolo supporto non contiene un insieme di file autonomamente intelligibile. Tale misura non costituisce cifratura a riposo.
- Cifratura a riposo dei supporti di produzione: misura pianificata, con completamento previsto entro il 30 giugno 2027.
- Dismissione dei supporti: nessun supporto di memorizzazione lascia l'infrastruttura in condizione leggibile. I supporti sostituiti sono sottoposti a distruzione fisica o cancellazione certificata prima della restituzione o dello smaltimento, con annotazione in apposito registro.

B.5 Backup, continuità e conservazione

Elemento	Configurazione
Copia primaria	Su infrastruttura iWebLab presso il sito di produzione
Copia off-site	Copia cifrata conservata presso fornitore ubicato in Germania (SEE)
Retention copie di sicurezza	Secondo il piano attivo, come indicato nella scheda tecnica del Servizio; alla scadenza la cancellazione è definitiva e irreversibile
Log tecnici (access ed error log)	Fino a 51 giorni: 21 giorni su filesystem, quindi nelle copie di sicurezza fino alla loro rotazione a 30 giorni
Log di sicurezza	Coincidono con i log tecnici (access ed error log): fino a 51 giorni
Log del servizio CDN	10 giorni, mediante rotazione sui punti di presenza; non inclusi nelle copie di sicurezza
Log di accesso amministrativo	90 giorni, su sistema di raccolta centralizzato esterno ai nodi di produzione

Elemento	Configurazione
RTO / RPO	Hosting condiviso e posta elettronica: RPO 12 ore (due copie di sicurezza giornaliere), obiettivo di ripristino del singolo account entro 8 ore dalla richiesta. VPS e server dedicati: RPO secondo il servizio di backup attivato, obiettivo di ripristino entro 24 ore. Gli obiettivi di ripristino costituiscono obbligazioni di mezzi ai sensi dell'art. 9.4 delle Condizioni Generali.
Verifica dei ripristini	Test di ripristino trimestrali, documentati

La retention effettiva dei log è pari al periodo di rotazione su filesystem sommato alla permanenza nelle copie di sicurezza. Va dichiarato il valore reale, non quello nominale.

B.6 Analisi automatizzata dei log per finalità di sicurezza

iWebLab impiega sistemi di analisi automatizzata basati su tecniche di apprendimento automatico, applicati esclusivamente agli access log e agli error log del server web, per il rilevamento di intrusioni, attività malevole e anomalie di sicurezza. Garanzie applicate:

- non è impiegato alcun fornitore terzo di servizi di intelligenza artificiale; l'elaborazione avviene integralmente su sistemi di proprietà di iWebLab, ubicati nella propria infrastruttura e non esposti alla rete pubblica;
- nessun dato è trasmesso a servizi esterni né reso disponibile a terzi;
- i modelli di rilevamento sono aggiornati sui pattern di traffico osservati sull'infrastruttura di iWebLab, in quanto l'adattamento alle tecniche di attacco emergenti è condizione necessaria all'efficacia della misura; tale addestramento avviene esclusivamente su sistemi di iWebLab e per la sola finalità di sicurezza. Nessun dato è impiegato per l'addestramento di modelli di terzi né per finalità diverse;
- i modelli incorporano pattern statistici aggregati e non consentono l'identificazione di singoli interessati né la ricostruzione dei record originari;
- il trattamento non ha finalità di profilazione degli interessati; le azioni automatiche consistono in misure tecniche di protezione reversibili, soggette a revisione da parte del personale;
- una policy interna vieta al personale l'inserimento di dati personali dei clienti in strumenti di intelligenza artificiale generativa esterni.

Gli access log possono contenere parametri di richiesta trasmessi dalle applicazioni del Cliente, ivi comprese, in taluni casi, credenziali di accesso a webservice trasmesse in query string. iWebLab applica mascheramento dei parametri riconducibili a credenziali prima dell'inserimento nelle copie di sicurezza e nel processo di analisi, e raccomanda al Cliente l'adozione di autenticazione basata su intestazioni HTTP, non soggetta a registrazione nei log.

B.7 Sicurezza applicativa e operativa

- Isolamento dei processi per singolo host virtuale sull'infrastruttura web.
- Filtraggio antispam e antivirus sul flusso di posta.
- Gestione degli aggiornamenti di sicurezza dei sistemi operativi e dei componenti dello stack.
- Monitoraggio della disponibilità, delle prestazioni e degli eventi di sicurezza.
- Mitigazione degli attacchi volumetrici e applicativi a livello perimetrale e di edge.
- Procedura documentata di gestione delle violazioni di dati personali, con notifica al Cliente entro 48 ore dalla presa di conoscenza.
- Policy interna sull'uso di strumenti di intelligenza artificiale e procedura di dismissione dei supporti di memorizzazione.

B.8 Misure a carico del Cliente

Il livello di sicurezza complessivo dipende anche dalla corretta gestione applicativa da parte del Cliente, cui competono in particolare:

- l'aggiornamento tempestivo di CMS, temi, plugin ed estensioni;
- la gestione delle utenze applicative, l'adozione di credenziali robuste e l'attivazione dell'autenticazione a più fattori ove disponibile;
- la configurazione delle integrazioni verso webservice secondo modalità che non espongano credenziali in query string;
- la definizione delle regole di caching per le pagine che veicolano contenuti personalizzati o riservati;
- la rotazione delle credenziali applicative in caso di sospetta compromissione;
- la corretta configurazione dei consensi e delle informative sui siti ospitati.

B.9 Nodi ubicati al di fuori dello Spazio Economico Europeo

Il servizio di distribuzione dei contenuti e il servizio di risoluzione DNS autorevole si avvalgono anche di nodi ubicati negli Stati Uniti d'America, indicati in Allegato C.

Su tali nodi sono trattati: i dati tecnici delle connessioni ricevute, ivi compreso l'indirizzo IP del richiedente o una porzione di esso; le richieste di risoluzione dei nomi a dominio; e, limitatamente ai nodi di distribuzione dei contenuti, copia temporanea in memoria e su disco delle risorse pubblicamente accessibili dei siti del Cliente.

Le connessioni fra il visitatore e il nodo, e fra il nodo e l'infrastruttura di origine, sono protette da cifratura in transito. I dati sono conservati sui nodi per il tempo strettamente necessario all'erogazione del servizio e secondo i periodi indicati alla sezione B.5.

L'elenco aggiornato dei nodi, con ubicazione e fornitore, è pubblicato all'indirizzo indicato in copertina ed è identificato dalla propria impronta informatica.

Allegato C — Sub-responsabili

Elenco alla data di emissione. La versione aggiornata è pubblicata all'indirizzo indicato in copertina e prevale in caso di difformità. I sub-responsabili si applicano al singolo Cliente limitatamente ai Servizi effettivamente attivati.

C.1 Sub-responsabili autorizzati

Soggetto	Paese	Attività	Servizio interessato
Hetzner Online GmbH	Germania	Conservazione della copia di sicurezza off-site cifrata	Backup
Hetzner Online GmbH	Germania	Punto di presenza CDN nel SEE	CDN
Hetzner Online GmbH	Germania / Finlandia	Nodi di risoluzione DNS autorevole nel SEE	DNS
Hetzner Online GmbH	Stati Uniti	Nodo di risoluzione DNS autorevole	DNS
OVH US LLC	Stati Uniti	Punto di presenza CDN	CDN

Soggetto	Paese	Attività	Servizio interessato
DigitalOcean, LLC	Stati Uniti	Nodo di risoluzione DNS autorevole	DNS
Aruba S.p.A.	Italia	Punto di presenza CDN nel SEE	CDN

I nodi ubicati negli Stati Uniti d'America trattano dati personali riferibili ai visitatori dei siti del Cliente e ai richiedenti la risoluzione dei nomi a dominio, secondo quanto descritto in Allegato B, sezione 9. Gli strumenti di trasferimento applicabili a ciascun fornitore sono indicati in Allegato D, sezione D.9. L'indirizzo di OVH US LLC è 11950 Democracy Drive, Suite 300, Reston, VA 20190, Stati Uniti d'America.

C.2 Fornitori che non trattano dati personali

I seguenti soggetti non rivestono la qualifica di sub-responsabile, in quanto non compiono operazioni su dati personali per conto di iWebLab:

Soggetto	Motivazione
HOST S.p.A. — Torino	Eroga esclusivamente spazio rack, alimentazione elettrica e connettività. Gli apparati sono di proprietà di iWebLab; il fornitore non dispone di credenziali amministrative né di accesso logico ai sistemi. L'accesso fisico è presidiato dalle misure di cui all'Allegato B, sezione 1.

C.3 Soggetti terzi autonomi

I registri di assegnazione dei nomi a dominio (Registro .it, registri gTLD e ccTLD, e i soggetti da questi accreditati) operano quali titolari autonomi del trattamento in relazione ai dati di registrazione, in adempimento delle rispettive policy e degli obblighi derivanti dai contratti con ICANN, ivi compresa la pubblicazione mediante i servizi RDAP e WHOIS secondo le regole applicabili a ciascuna estensione. iWebLab trasmette a tali soggetti i dati necessari alla registrazione e al mantenimento dei nomi a dominio su istruzione del Cliente. Il Cliente è tenuto a informare gli interessati di tale comunicazione.

Allegato D — Valutazione d'impatto sul trasferimento

Transfer Impact Assessment — clausola 14 delle SCC e Raccomandazioni EDPB 01/2020

D.1 Oggetto e metodo

La presente valutazione esamina se il quadro giuridico e le prassi della Repubblica di San Marino impediscano all'importatore di adempiere agli obblighi assunti con le SCC, e se siano necessarie misure supplementari ai sensi delle Raccomandazioni EDPB 01/2020. L'analisi segue le sei fasi ivi previste.

D.2 Fase 1 — Mappatura del trasferimento

Elemento	Descrizione
Esportatore	Il Cliente, stabilito nello Spazio Economico Europeo
Importatore	iWebLab S.r.l., Repubblica di San Marino
Natura del trasferimento	Accesso remoto ai dati da parte del personale tecnico dell'importatore per finalità di amministrazione, manutenzione e sicurezza
Ubicazione fisica dei dati	Spazio Economico Europeo (Italia per la produzione, Germania per la copia off- site cifrata)

Elemento	Descrizione
Categorie di dati	Come da Allegato A
Categorie di interessati	Come da Allegato A
Finalità	Erogazione e sicurezza dei Servizi
Trasferimenti successivi	Punto di presenza CDN negli Stati Uniti (OVH US LLC), limitato al traffico dei crawler; cfr. sezione D.9

Elemento rilevante ai fini della valutazione: i dati non sono fisicamente esportati verso il paese terzo. Il trasferimento consiste esclusivamente nella possibilità di accesso remoto da San Marino a dati che permangono su infrastruttura ubicata nel SEE. Le autorità sammarinesi non dispongono pertanto di giurisdizione territoriale sui supporti su cui i dati risiedono.

D.3 Fase 2 — Strumento di trasferimento utilizzato

Clausole Contrattuali Tipo adottate con Decisione di esecuzione (UE) 2021/914, Modulo 2 o Modulo 3 secondo la qualificazione delle Parti, ai sensi dell'art. 46, par. 2, lett. c) GDPR.

D.4 Fase 3 — Valutazione del quadro giuridico del paese terzo

D.4.1 Quadro generale in materia di protezione dei dati

- La Repubblica di San Marino dispone di una disciplina organica in materia di protezione dei dati personali, recata dalla Legge 21 dicembre 2018 n. 171, adottata al dichiarato fine di allineare l'ordinamento interno ai principi del Regolamento (UE) 2016/679.
- La legge riconosce i principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza, nonché i diritti degli interessati corrispondenti a quelli previsti dal Capo III GDPR.
- È istituita un'Autorità Garante per la protezione dei dati personali, dotata di indipendenza e di poteri di controllo, indagine e sanzione.
- La Repubblica di San Marino ha aderito alla Convenzione n. 108 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale.

D.4.2 Tutela giurisdizionale e diritti fondamentali

- La Repubblica di San Marino è membro del Consiglio d'Europa e parte della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali; gli interessati dispongono pertanto del ricorso alla Corte europea dei diritti dell'uomo previo esaurimento dei rimedi interni.
- L'ordinamento sammarinese garantisce l'indipendenza della magistratura e il diritto a un ricorso effettivo dinanzi a un'autorità giurisdizionale.
- Gli interessati dispongono di rimedi amministrativi dinanzi all'Autorità Garante e di rimedi giurisdizionali per il risarcimento del danno.

D.4.3 Accesso ai dati da parte delle autorità pubbliche

- L'ordinamento sammarinese non prevede programmi di sorveglianza massiva né obblighi generalizzati di accesso o di collaborazione a carico dei fornitori di servizi di comunicazione elettronica assimilabili a quelli oggetto delle pronunce della Corte di giustizia nelle cause C-362/14 e C-311/18.
- L'accesso delle autorità ai dati è consentito nell'ambito di procedimenti penali o di indagini specifiche, previa autorizzazione dell'autorità giudiziaria, secondo i presupposti e i limiti stabiliti dalla legge.

- L'assistenza giudiziaria internazionale è prestata secondo gli strumenti convenzionali applicabili, che prevedono il vaglio dell'autorità giudiziaria interna.
- Non risultano, alla data della presente valutazione, obblighi di legge che impongano all'importatore di consentire un accesso indiscriminato ai dati trattati per conto di clienti esteri, né divieti di informare l'esportatore di eventuali richieste ricevute, salvi i limiti ordinari del segreto istruttorio.

D.4.4 Esperienza dell'importatore iWebLab dichiara che, alla data della presente valutazione, non ha ricevuto da autorità pubbliche sammarinesi o di altri Stati richieste di accesso a dati personali trattati per conto dei propri clienti. iWebLab tiene un registro delle eventuali richieste ricevute e si impegna a darne comunicazione all'esportatore nei limiti consentiti dalla legge, come previsto dalle clausole 15.1 e 15.2 delle SCC.

D.5 Fase 4 — Valutazione rispetto alle European Essential Guarantees

Si applicano le quattro garanzie essenziali europee elaborate dall'EDPB (Raccomandazioni 02/2020):

#	Garanzia Valutazione
1	Il trattamento deve fondarsi su norme Soddisfatta. L'accesso ai dati da parte delle autorità è chiare, precise e accessibili disciplinato da norme di rango primario, pubbliche e accessibili, che ne definiscono presupposti e limiti.
2	Devono essere dimostrate necessità e Soddisfatta. L'accesso è ammesso per finalità determinate di proporzionalità prevenzione e repressione dei reati, subordinatamente a un vaglio di necessità nel caso concreto. Non sono previsti programmi di raccolta generalizzata.
3	Deve esistere un meccanismo di Soddisfatta. L'accesso è soggetto ad autorizzazione controllo indipendente dell'autorità giudiziaria; opera inoltre un'autorità di controllo indipendente in materia di protezione dei dati.
#	Garanzia Valutazione
4	Devono essere disponibili rimedi effettivi Soddisfatta. Gli interessati dispongono di rimedi per gli interessati amministrativi dinanzi all'Autorità Garante, di rimedi giurisdizionali interni e del ricorso alla Corte EDU.

D.6 Fase 5 — Conclusione e misure supplementari

Alla luce di quanto precede, iWebLab ritiene che il quadro giuridico e le prassi della Repubblica di San Marino non impediscano l'adempimento degli obblighi assunti con le SCC e non pregiudichino il livello di protezione garantito dal diritto dell'Unione. Non si ravvisa pertanto la necessità di misure supplementari ai sensi delle Raccomandazioni EDPB 01/2020. Elemento ulteriormente rilevante è che i dati non risiedono nel paese terzo: essi permangono su infrastruttura ubicata nello Spazio Economico Europeo, e il trasferimento si esaurisce nella possibilità di accesso remoto. Un'eventuale richiesta di un'autorità sammarinese non avrebbe pertanto ad oggetto supporti soggetti alla sua giurisdizione territoriale. Ancorché non necessarie, iWebLab adotta comunque, quali misure di difesa in profondità, le seguenti:

- accesso amministrativo limitato a personale nominativamente individuato, da postazioni autorizzate, con autenticazione a più fattori e tracciamento delle operazioni;
- cifratura dei canali di accesso e delle copie di sicurezza off-site;
- ubicazione dell'infrastruttura di produzione e delle copie di sicurezza nello Spazio Economico Europeo;
- impegno contrattuale a contestare in sede giurisdizionale le richieste di accesso manifestamente illegittime e a informare l'esportatore nei limiti consentiti dalla legge;
- tenuta di un registro delle richieste di accesso ricevute da autorità pubbliche.

D.7 Fase 6 — Attuazione

Le misure descritte sono attuate e documentate negli Allegati B e C del presente accordo.

D.8 Riesame

La presente valutazione è riesaminata almeno ogni dodici mesi, nonché ogni volta che iWebLab abbia notizia di modifiche normative o di prassi rilevanti nel paese terzo, ovvero riceva una richiesta di accesso da parte di un'autorità pubblica. La Repubblica di San Marino persegue l'adozione di una decisione di adeguatezza ai sensi dell'art. 45 GDPR. Ove tale decisione intervenisse, il ricorso alle SCC per il trasferimento verso iWebLab non sarebbe più necessario e il presente accordo sarebbe aggiornato di conseguenza. Resterebbe comunque necessario l'accordo ex art. 28 GDPR.

D.9 Trasferimenti verso gli Stati Uniti d'America

Ai fini della clausola 8.8 delle SCC si dà conto dei seguenti trasferimenti successivi.

Destinatario	Ruolo	Dati trattati	Strumento di trasferimento
OVH US LLC — Reston, Virginia	Punto di presenza CDN	Dati tecnici di connessione dei visitatori, ivi compreso l'indirizzo IP; copia delle risorse pubblicamente accessibili dei siti	Clausole Contrattuali Tipo, Modulo 3, allegate al contratto del fornitore
Hetzner Online GmbH — nodo statunitense	Nodo di risoluzione DNS autorevole	Indirizzo IP, o porzione di esso, del richiedente la risoluzione; dati tecnici di connessione	In corso di formalizzazione; la presente sezione è aggiornata all'esito, con comunicazione ai sensi dell'art. 15
DigitalOcean, LLC — Santa Clara, California	Nodo di risoluzione DNS autorevole	Indirizzo IP, o porzione di esso, del richiedente la risoluzione; dati tecnici di connessione	In corso di formalizzazione; la presente sezione è aggiornata all'esito, con comunicazione ai sensi dell'art. 15

Valutazione. I nodi ubicati negli Stati Uniti trattano dati personali riferibili ai visitatori dei siti del Cliente e ai richiedenti la risoluzione dei nomi a dominio. Il trattamento è funzionalmente necessario all'erogazione dei servizi richiesti dal Cliente e non è eliminabile senza rinunciare al servizio, salvo quanto previsto all'art. 11.4.

I dati trattati su tali nodi sono di natura tecnica e di norma non consentono, da soli, l'identificazione diretta dell'interessato; sono conservati per i periodi indicati in Allegato B, sezione B.5, e protetti da cifratura in transito.

Tenuto conto della natura dei dati, della loro conservazione limitata e delle garanzie contrattuali in essere con ciascun fornitore, iWebLab ritiene che il livello di protezione sia sostanzialmente equivalente a quello garantito nello Spazio Economico Europeo. La presente valutazione è riesaminata ad ogni variazione dei nodi, dei fornitori o degli strumenti di trasferimento.

Appendice — Allegati alle Clausole Contrattuali Tipo

Decisione di esecuzione (UE) 2021/914 — Modulo 2 (titolare a responsabile) o Modulo 3 (responsabile a sub-responsabile), secondo la qualificazione delle Parti ai sensi dell'art. 2 dell'accordo.

Allegato I.A — Elenco delle parti

Parte	Dati identificativi
Esportatore	Il Cliente, come identificato nel contratto di servizio e nell'area riservata. Attività rilevanti: acquisizione di servizi di hosting e connessi. Ruolo: titolare del trattamento ovvero responsabile del trattamento, secondo quanto previsto dall'art. 2 dell'accordo.
Importatore	iWebLab S.r.l., Strada Nona Guladaria 68, 47895 Domagnano, Repubblica di San Marino, COE SM30107. Referente: Giuseppe Semeraro, [email]. Attività rilevanti: erogazione dei Servizi di cui all'Allegato A. Ruolo: responsabile del trattamento ovvero sub-responsabile.

Allegato I.B — Descrizione del trasferimento

Elemento	Riferimento
Categorie di interessati	Allegato A, sezione A.4
Categorie di dati personali	Allegato A, sezione A.3
Categorie particolari di dati	Non previste, salvo preventivo accordo scritto ai sensi dell'art. 14 dell'accordo
Frequenza del trasferimento	Continuativa, per la durata del rapporto contrattuale
Natura del trattamento	Allegato A, sezione A.1
Finalità	Allegato A, sezione A.2
Periodo di conservazione	Art. 12 dell'accordo e Allegato B, sezione B.5
Trasferimenti a sub-responsabili	Allegato C. Alcuni sub-responsabili sono ubicati negli Stati Uniti d'America, per i servizi di distribuzione dei contenuti e di risoluzione DNS autorevole; cfr. art. 11.4 e Allegato D, sezione D.9

Opzioni esercitate nelle SCC

Clausola	Opzione
7 — Adesione	Inclusa: ulteriori soggetti possono aderire alle Clausole con il consenso delle Parti
9 — Sub-responsabili	Opzione 2, autorizzazione generale, con preavviso di 30 giorni come previsto dall'art. 7 dell'accordo
11 — Mezzi di ricorso	Opzione facoltativa non inclusa
13 — Autorità di controllo	Come indicato nell'Allegato I.C
17 — Legge applicabile	Opzione 1: legge della Repubblica Italiana

Clausola	Opzione
Clausola	Opzione
18 — Foro competente	Giudici della Repubblica Italiana, Foro di Rimini, salvo la facoltà degli interessati di cui alla lettera c)

Allegato I.C — Autorità di controllo competente

L'autorità di controllo competente è individuata ai sensi della clausola 13 delle SCC: l'autorità dello Stato membro in cui è stabilito l'esportatore, ovvero, per gli esportatori non stabiliti nell'Unione ma soggetti al GDPR ai sensi dell'art. 3, par. 2, l'autorità dello Stato membro in cui è stabilito il rappresentante designato ai sensi dell'art. 27 GDPR.

Allegato II — Misure tecniche e organizzative Le misure tecniche e organizzative adottate dall'importatore, comprese quelle volte a garantire la sicurezza dei dati, sono descritte nell'Allegato B del presente accordo, che si intende qui integralmente richiamato.

Sub-responsabili (informativa) Essendo esercitata l'opzione 2 della clausola 9 (autorizzazione generale), l'Allegato III delle SCC non è compilato. A fini informativi, l'elenco dei sub-responsabili è riportato nell'Allegato C del presente accordo ed è pubblicato, nella versione aggiornata, all'indirizzo indicato in copertina.