Data Processing Agreement

Accordo sul Trattamento dei Dati Personali
ai sensi dell'art. 28 del Regolamento UE 2016/679 (GDPR)

HB-DPA-2026-XXX | Rev. 1.2 — 2026 | Rif. contratto: [Riferimento contratto / offerta]

Responsabile del Trattamento

HyperBit SRLs
Via dei Prati 41/B, 38057, Pergine Valsugana (TN), Italia
P.IVA / CF: IT02697330229 · REA: TN-243469
privacy@hyperbit.it
cert@pec.hyperbit.it

Titolare del Trattamento

[Ragione Sociale Cliente S.r.l.]
[Indirizzo Cliente, CAP, Città (Provincia)]
IT[XXXXXXXXXXX]
[referente@cliente.it]

Il presente accordo disciplina il trattamento dei dati personali effettuato da HyperBit SRLs in qualità di Responsabile del Trattamento per conto del Cliente, in relazione ai servizi oggetto del contratto di riferimento ([Riferimento contratto / offerta]). Costituisce parte integrante e allegato obbligatorio al contratto di servizio.

1 Premesse e Definizioni

Le parti hanno stipulato un contratto di servizio (rif. [Riferimento contratto / offerta]) in virtù del quale HyperBit SRLs (di seguito “Responsabile”) eroga al Cliente (di seguito “Titolare”) servizi che comportano il trattamento di dati personali per conto del Titolare stesso.

Ai sensi dell’art. 28 del Regolamento UE 2016/679 (di seguito “GDPR”), il trattamento da parte di un Responsabile deve essere disciplinato da un contratto o altro atto giuridico vincolante. Il presente Accordo costituisce tale atto.

1.1 Definizioni

Ai fini del presente Accordo si applicano le definizioni di cui all’art. 4 GDPR. In particolare:

- “Dati Personali”: qualsiasi informazione riguardante una persona fisica identificata o identificabile.
- “Trattamento”: qualsiasi operazione o insieme di operazioni eseguita sui Dati Personali.
- “Titolare del Trattamento”: il Cliente che determina finalità e mezzi del trattamento.
- “Responsabile del Trattamento”: HyperBit SRLs, che tratta i Dati Personali per conto del Titolare.
- “Sub-Responsabile”: soggetto terzo nominato dal Responsabile per eseguire specifiche attività di trattamento.
- “Interessato”: la persona fisica cui si riferiscono i Dati Personali.
- “Violazione dei Dati” (data breach): violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai Dati Personali.
- “Autorità di Controllo”: il Garante per la Protezione dei Dati Personali (Italia).

Art. 1 — Oggetto, Natura e Istruzioni del Trattamento

Il Responsabile tratta i Dati Personali esclusivamente per conto e su istruzione documentata del Titolare, nell'ambito dell'erogazione dei seguenti servizi:

Servizio	Natura del trattamento
Connettività ISP	Trasmissione dati, gestione accessi di rete, logging traffico, autenticazione RADIUS/AAA, assegnazione IP.
Managed Security (MSSP)	Raccolta e analisi log di sicurezza, monitoraggio XDR/SIEM (SentinelOne + Microsoft Sentinel), rilevamento e risposta a incidenti, threat intelligence, gestione alert.
Managed Service Provider (MSP)	Gestione endpoint, backup, Microsoft 365/Intune, helpdesk, accesso remoto ai sistemi del Titolare per finalità di manutenzione e supporto.

Il Responsabile non tratta i Dati Personali per finalità proprie, diverse da quelle indicate dal Titolare, salvo obbligo di legge, nel qual caso ne dà tempestiva comunicazione al Titolare (salvo divieto di legge).

Qualsiasi istruzione aggiuntiva del Titolare deve essere fornita per iscritto. Se il Responsabile ritiene che un'istruzione violi il GDPR o altra normativa applicabile, ne informa prontamente il Titolare.

Art. 2 — Categorie di Dati Personali e Interessati

Categoria	Dettaglio
Dati anagrafici	Nome, cognome, indirizzo e-mail, numero di telefono, ruolo aziendale degli utenti/dipendenti del Titolare.
Dati di traffico di rete	Indirizzi IP, timestamp, protocolli, volumi di traffico, DNS query, log di connessione.
Log di autenticazione	Credenziali hash, MAC address, eventi RADIUS/AAA, timestamp login/logout.
Dati di sicurezza (XDR/SIEM)	Alert di sicurezza, IoC, eventi policy violation, log endpoint, telemetria SentinelOne, eventi Microsoft Sentinel.
Dati di sistema (MSP)	Log applicativi, configurazioni, backup di dati aziendali, eventi di accesso remoto.

Categorie di interessati: dipendenti, collaboratori, utenti e clienti del Titolare che utilizzano i servizi oggetto del contratto.

Il Responsabile non tratta categorie particolari di dati (art. 9 GDPR) né dati relativi a condanne penali (art. 10 GDPR) salvo istruzione scritta e documentata del Titolare, previa verifica della sussistenza di idonea base giuridica.

Art. 3 — Obblighi del Responsabile

Il Responsabile si impegna a:

3.1 Riservatezza e personale autorizzato

Trattare i Dati Personali esclusivamente attraverso persone autorizzate al trattamento, vincolate da obbligo di riservatezza contrattuale o per legge. Il Responsabile garantisce che il personale autorizzato abbia ricevuto adeguata formazione in materia di protezione dei dati.

3.2 Misure di sicurezza (art. 32 GDPR)

Adottare e mantenere misure tecniche e organizzative adeguate a garantire un livello di sicurezza proporzionato al rischio, tra cui:

- Crittografia dei dati in transito (TLS 1.2+) e a riposo per i dati sensibili.
- Autenticazione a più fattori (MFA) per l'accesso ai sistemi di gestione.
- Segmentazione di rete e principio del minimo privilegio.
- Monitoraggio continuo tramite SentinelOne XDR e Microsoft Sentinel.
- Backup cifrati su Wasabi EU (Object Lock, policy 3-2-1) con RTO/RPO definiti.
- Audit e vulnerability assessment periodici sull'infrastruttura.
- Infrastruttura principale presso Seeweb Milano Caldera (Tier III, ISO 27001).

3.3 Assistenza al Titolare

Assistere il Titolare, nei limiti del possibile e con oneri a carico del Titolare per attività eccedenti il normale perimetro contrattuale, nell'adempimento degli obblighi di:

- risposta alle richieste di esercizio dei diritti degli interessati (artt. 15–22 GDPR);
- notifica e comunicazione di violazioni dei dati (artt. 33–34 GDPR);
- esecuzione di Valutazioni d'Impatto sulla Protezione dei Dati (DPIA, art. 35 GDPR);
- consultazione preventiva con l'Autorità di Controllo (art. 36 GDPR).

3.4 Finalità esclusiva

Non trattare i Dati Personali per finalità proprie o diverse da quelle istruite dal Titolare, né cederli a terzi al di fuori dei casi previsti dal presente Accordo o dalla legge.

3.5 Cancellazione o restituzione

Alla cessazione del contratto di servizio, cancellare o restituire al Titolare tutti i Dati Personali trattati per suo conto, a scelta del Titolare, entro 30 giorni dalla cessazione, e cancellare le eventuali copie esistenti, salvo obbligo di conservazione previsto dalla legge (es. D.Lgs. 109/2008 per i dati di traffico).

3.6 Audit e dimostrabilità

Mettere a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi di cui al presente Accordo e consentire e contribuire alle attività di audit e ispezione effettuate dal Titolare o da un soggetto da questi incaricato, con preavviso scritto di almeno 15 giorni lavorativi e nei limiti della riservatezza delle informazioni di terzi.

Art. 4 — Nomina dei Sub-Responsabili

Il Titolare autorizza il Responsabile ad avvalersi dei seguenti Sub-Responsabili per l'esecuzione di specifiche attività di trattamento:

Sub-Responsabile	Sede / Paese	Attività di trattamento
Seeweb S.r.l.	Italia (Milano)	Colocation e infrastruttura di rete — POP principale AS208437.
Revolution Provider S.r.l.	Italia (Milano)	Transito IP e infrastruttura di rete L2.
RETN S.r.l.	Italia (Milano)	Transito IP.
Bicom Systems (ZeroZero 39 SRL)	Italia (Firenze)	Centralino VoIP
SentinelOne Inc.	UE (elaborazione dati EU)	Piattaforma XDR — rilevamento e risposta endpoint.
Aruba S.p.A.	Italia (Milano)	Infrastruttura di rete e Macchine Virtuali
Hetzner Online GmbH	UE (Germania)	Macchine Virtuali
Scaleway SAS	UE (Francia)	Email Transazionale / Database
Microsoft Ireland Operations Ltd.	Irlanda / UE	Microsoft Sentinel (SIEM), Microsoft 365, Intune — gestione cloud e sicurezza, Microsoft XDR, Microsoft Azure.
Wasabi Technologies	UE (Amsterdam)	Storage immutabile per backup cifrati (Object Lock).

Il Responsabile impone ai Sub-Responsabili obblighi equivalenti a quelli previsti nel presente Accordo mediante contratto scritto. Il Responsabile rimane pienamente responsabile nei confronti del Titolare per l'adempimento degli obblighi dei Sub-Responsabili.

Il Responsabile informa il Titolare di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di Sub-Responsabili, tramite comunicazione scritta a [referente@cliente.it] con preavviso di almeno 30 giorni. Il Titolare ha il diritto di opporsi a tali modifiche entro tale termine; in mancanza di opposizione, le modifiche si intendono accettate.

Trasferimenti extra-UE: qualora un Sub-Responsabile tratti dati al di fuori dell'UE/SEE, il Responsabile garantisce che il trasferimento avvenga nel rispetto del Capo V GDPR (decisione di adeguatezza, SCC, BCR). Documentazione disponibile su richiesta scritta a privacy@hyperbit.it.

Art. 5 — Gestione delle Violazioni dei Dati Personali

5.1 Il Responsabile notifica al Titolare qualsiasi violazione dei dati personali (data breach) di cui venga a conoscenza, senza ingiustificato ritardo e, ove possibile, entro 24 ore dalla scoperta, al seguente contatto: [referente@cliente.it].

5.2 La notifica contiene almeno:

- Descrizione della natura della violazione, con indicazione delle categorie e del numero approssimativo di interessati e di registrazioni di dati coinvolte.
- Nome e dati di contatto del DPO o di altro punto di contatto.
- Descrizione delle probabili conseguenze della violazione.
- Descrizione delle misure adottate o proposte per porre rimedio alla violazione, incluse le misure per attenuarne i possibili effetti negativi.

5.3 Il Responsabile assiste il Titolare nella notifica della violazione all'Autorità di Controllo (art. 33 GDPR, entro 72 ore) e, ove applicabile, nella comunicazione agli interessati (art. 34 GDPR).

5.4 Il Responsabile documenta tutte le violazioni dei dati, incluse quelle non soggette a obbligo di notifica, e ne trasmette il registro al Titolare su richiesta.

Art. 6 — Assistenza nell'Esercizio dei Diritti degli Interessati

6.1 Qualora il Responsabile riceva direttamente una richiesta di esercizio dei diritti da parte di un interessato (artt. 15–22 GDPR), la inoltra senza ritardo al Titolare e non vi dà corso autonomamente, salvo istruzione scritta del Titolare.

6.2 Il Responsabile fornisce al Titolare, su richiesta e nei limiti delle proprie possibilità tecniche, le informazioni e l'assistenza necessarie per consentire al Titolare di rispondere all'interessato entro i termini previsti dal GDPR (30 giorni, prorogabili di ulteriori 60 giorni in casi complessi).

6.3 Il Responsabile implementa, ove tecnicamente fattibile, meccanismi per supportare le richieste di cancellazione, portabilità, limitazione e opposizione, in modo coordinato con le istruzioni del Titolare.

Art. 7 — Riservatezza

7.1 Il Responsabile mantiene riservati i Dati Personali trattati per conto del Titolare e garantisce che il proprio personale e i Sub-Responsabili siano vincolati da idonei obblighi di riservatezza.

7.2 L'obbligo di riservatezza permane anche successivamente alla cessazione del presente Accordo e del contratto di servizio correlato, senza limiti di tempo, per quanto riguarda i Dati Personali del Titolare.

7.3 Il Responsabile comunica i Dati Personali a terzi solo nei casi previsti dal presente Accordo, su istruzione documentata del Titolare, o in adempimento di obbligo di legge (es. richieste dell'Autorità Giudiziaria ai sensi del D.Lgs. 109/2008), informando il Titolare ove possibile e consentito dalla legge.

Art. 8 — Durata e Cessazione

8.1 Il presente Accordo entra in vigore alla data di sottoscrizione e ha la stessa durata del contratto di servizio di riferimento ([Riferimento contratto / offerta]).

8.2 Alla cessazione del contratto di servizio, per qualsiasi causa, il Responsabile — salvo diversa istruzione scritta del Titolare — procede entro 30 giorni a:

- cancellare in modo sicuro tutti i Dati Personali trattati per conto del Titolare dai propri sistemi e dai sistemi dei Sub-Responsabili;
- fornire al Titolare attestazione scritta dell'avvenuta cancellazione;
- restituire, su richiesta del Titolare, copia dei Dati Personali in formato strutturato e leggibile da dispositivo automatico.

8.3 Gli obblighi di riservatezza (art. 7) e le disposizioni in materia di responsabilità (art. 9) sopravvivono alla cessazione del presente Accordo.

8.4 Eventuali obblighi legali di conservazione (es. D.Lgs. 109/2008 per i dati di traffico) prevalgono sugli obblighi di cancellazione, limitatamente ai dati e ai periodi previsti dalla legge. Il Responsabile ne informa il Titolare per iscritto.

Art. 9 — Responsabilità

9.1 Il Responsabile è responsabile nei confronti del Titolare per i danni causati dal trattamento in violazione degli obblighi previsti dal presente Accordo o dal GDPR, imputabili al Responsabile.

9.2 Il Responsabile è esonerato da responsabilità qualora dimostri che l'evento dannoso non gli è in alcun modo imputabile ai sensi dell'art. 82 par. 3 GDPR.

9.3 In caso di azione legale di un interessato o dell'Autorità di Controllo nei confronti del Responsabile per fatti riconducibili a istruzioni errate o incomplete del Titolare, quest'ultimo tiene indenne il Responsabile da ogni conseguente pregiudizio economico.

9.4 La responsabilità del Responsabile per danni indiretti, perdita di dati, mancato guadagno o danno reputazionale è esclusa, salvo dolo o colpa grave.

Art. 10 — Legge Applicabile e Foro Competente

10.1 Il presente Accordo è regolato dalla legge italiana, incluso il D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018, e dal GDPR.

10.2 Per qualsiasi controversia relativa all'interpretazione, validità o esecuzione del presente Accordo, le parti eleggono la competenza esclusiva del Tribunale di Trento.

10.3 Le parti si impegnano a tentare una risoluzione amichevole della controversia entro 30 giorni dalla comunicazione scritta della parte che la solleva, prima di adire l'Autorità Giudiziaria.

Art. 11 — Disposizioni Finali

11.1 Il presente Accordo, unitamente al contratto di servizio ([Riferimento contratto / offerta]) e ai suoi allegati, costituisce l'integrale accordo tra le parti in materia di protezione dei dati personali e sostituisce ogni precedente intesa al riguardo.

11.2 Qualsiasi modifica al presente Accordo deve essere concordata per iscritto e sottoscritta da entrambe le parti.

11.3 Se una clausola del presente Accordo risultasse invalida o inapplicabile, le restanti clausole mantengono la loro validità ed efficacia. Le parti si impegnano a sostituire la clausola invalida con una valida che si avvicini il più possibile all'intento originario.

11.4 Il presente Accordo è redatto in lingua italiana. In caso di versione bilingue, la versione italiana prevale in caso di discrepanze.

2 Allegato A — Misure Tecniche e Organizzative (art. 32 GDPR)

Il presente allegato descrive le misure di sicurezza adottate da HyperBit SRLs in qualità di Responsabile del trattamento.

2.1 Misure tecniche

Area	Misura
Crittografia	TLS 1.2+ per tutti i dati in transito. Crittografia a riposo per backup e dati sensibili su Wasabi EU (AES-256).
Controllo accessi	MFA obbligatoria per tutti gli accessi ai sistemi di gestione. RBAC (Role-Based Access Control) con principio del minimo privilegio. Revisione trimestrale degli accessi.
Sicurezza di rete	Segmentazione VLAN, firewall perimetrale gestito, IDS/IPS. Monitoraggio traffico con NetFlow + Kentik. BGP filtering e RPKI per la sicurezza del routing (AS208437).
Rilevamento minacce	SentinelOne Singularity XDR su endpoint con risposta automatica e rollback. Microsoft Sentinel SIEM con Logic Apps per automazione. Threat intelligence multi-feed con correlazione cross-tenant.
Backup e DR	Policy 3-2-1: 3 copie, 2 supporti, 1 offsite (Wasabi EU). Object Lock per immutabilità. Backup incrementali giornalieri, full settimanali. RTO/RPO definiti per workload.
Infrastruttura fisica	POP principale presso Seeweb Milano Caldera: datacenter Tier III, certificazione ISO 27001, accesso fisico controllato con badge e CCTV.
Vulnerability management	Scansioni di vulnerability assessment periodiche. Patch management strutturato con finestre di manutenzione programmate. Penetration test annuale.

2.2 Misure organizzative

- Formazione periodica del personale su GDPR, protezione dei dati e cybersecurity.
- Procedure documentate di gestione degli incidenti e data breach response.
- Registro delle attività di trattamento (art. 30 GDPR) aggiornato.
- Accordi di riservatezza (NDA) con tutto il personale e i collaboratori.
- Revisione annuale delle misure di sicurezza e del presente Accordo.
- Procedura di onboarding/offboarding per la gestione degli accessi del personale.

3 Sottoscrizione

Le parti dichiarano di aver letto e compreso il presente Accordo e si obbligano al rispetto di quanto in esso contenuto.

Per il Responsabile del Trattamento
HyperBit SRLs

Nome e Cognome

Ruolo / Qualifica

Data e Firma

Luogo: Pergine Valsugana (TN)

Per il Titolare del Trattamento
[Ragione Sociale Cliente S.r.l.]

Nome e Cognome

Ruolo / Qualifica

Data e Firma

Luogo:

Artt. 1341–1342 c.c. — Clausole vessatorie: le parti dichiarano di approvare specificamente, ai sensi degli artt. 1341 e 1342 del Codice Civile, le seguenti clausole: Art. 9 (Responsabilità e limitazioni), Art. 10 (Foro competente esclusivo — Tribunale di Trento).

Firma per approvazione specifica:

Firma Responsabile

Firma Titolare

HyperBit SRLs · Via dei Prati 41/B, 38057, Pergine Valsugana (TN), Italia
P.IVA / CF: IT02697330229 · REA: TN-243469 · ROC: 42486
privacy@hyperbit.it · cert@pec.hyperbit.it · https://hyperbit.it