DATA PROCESSING AGREEMENT

CONTRATTO DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO (art. 28 GDPR)

PREMESSE

Host è una società attiva nel settore dei servizi di hosting. Offre ai propri clienti una serie di servizi in Cloud Computing, sia in modalità IaaS (Infrastructure as a Service), sia in modalità SaaS (Software as a Service).

Nel primo caso, mette a disposizione la propria infrastruttura, più precisamente i propri datacenter, per consentire l'hosting di dati, siti web, applicazioni software, server di proprietà del cliente e simili.

Nel secondo caso, Host fornisce una serie di servizi quali: posta elettronica e PEC; registrazione e gestione dei nomi a dominio; servizi antispam; strumenti per la protezione dei siti web, per garantirne la conformità alla normativa in materia di cookie o per migliorarne le prestazioni.

Nell'ambito dell'erogazione di questi servizi, Host potrà trattare dati di natura personale. **Anche nei casi in cui Host non può accedere ai dati personali, la mera conservazione effettuata sulle proprie infrastrutture costituisce un trattamento eseguito per conto di un titolare.** Tali trattamenti sono effettuati nel rispetto delle disposizioni del Regolamento (UE) 2016/679 (GDPR), in particolare dell'art. 28.

Nell'ipotesi in cui il cliente di Host non sia il titolare del trattamento ma sia a sua volta un soggetto responsabile, in tal caso Host assume il ruolo di sub-responsabile del trattamento. I rapporti fra responsabile e sub-responsabile sono anch'essi disciplinati da questo Data Processing Agreement.

Per semplicità, nel presente accordo i termini "Titolare" e "Responsabile" saranno utilizzati anche nei casi in cui Host agisca come responsabile del trattamento per conto di un cliente e il fornitore come sub-responsabile. In tali circostanze:

- il termine "Titolare" dovrà essere inteso come "Responsabile del trattamento",
- il termine "Responsabile" come "Sub-responsabile del trattamento".

Quando l'accordo è stipulato tra un responsabile e un sub-responsabile del trattamento, gli obblighi indicati nelle clausole 6 e 7 – che il GDPR attribuisce al titolare – si intendono, in questo contesto, come obblighi nei confronti del responsabile. Il sub-responsabile, nell'ambito del trattamento svolto, collabora con il responsabile dell'assistenza da prestare al titolare del trattamento.

Questo Data Processing Agreement costituisce un Addendum al contratto di servizi concluso in forma digitale fra Host e il cliente al momento dell'acquisto del servizio. In mancanza di un diverso accordo, le condizioni del presente Data Processing Agreement sono applicabili automaticamente a tutti i servizi erogati da Host che comportano trattamenti di dati da parte di quest'ultima in qualità di responsabile del trattamento.

SEZIONE I

1. Scopo e ambito di applicazione

a. Scopo del presente Data Processing Agreement è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 (GDPR).

b. I titolari del trattamento e i responsabili del trattamento di cui all'allegato I hanno accettato questo Data Processing Agreement al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679.

c. Questo Data Processing Agreement si applica al trattamento dei dati personali specificato all'allegato II.

d. Gli allegati da I a IV costituiscono parte integrante del Data Processing Agreement.

e. Il presente Data Processing Agreement lascia impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del regolamento (UE) 2016/679.

f. Il presente Data Processing Agreement non garantisce, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del regolamento (UE) 2016/679.

2. Interpretazione del Data Processing Agreement

a. Quando il Data Processing Agreement utilizza i termini definiti nel regolamento (UE) 2016/679, tali termini hanno lo stesso significato di cui al regolamento.

b. Il presente Data Processing Agreement va letto e interpretato alla luce delle disposizioni del regolamento (UE) 2016/679.

c. Il presente Data Processing Agreement non deve essere interpretato in un senso che non sia conforme ai diritti e agli obblighi previsti dal regolamento (UE) 2016/679, o che pregiudichi i diritti o le libertà fondamentali degli interessati.

3. Gerarchia

In caso di contraddizione tra il presente Data Processing Agreement e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione del presente Data Processing Agreement, o conclusi successivamente, prevale il Data Processing Agreement.

SEZIONE II - OBBLIGHI DELLE PARTI

4. Descrizione del trattamento

I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'allegato II.

5. Obblighi delle parti

5.1 Istruzioni

a. Il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.

b. Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il regolamento (UE) 2016/679 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

5.2 Limitazione delle finalità

Il responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato II, salvo ulteriori istruzioni del titolare del trattamento.

5.3 Durata del trattamento dei dati personali

Il responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'allegato II.

5.4 Sicurezza del trattamento

a. Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della

natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati. In particolare, considerato che il responsabile del trattamento opera come fornitore di servizi di hosting e non ha accesso al contenuto dei dati né visibilità sul tipo di trattamento effettuato, spetta al titolare del trattamento valutare la natura dei dati e il rischio ad essi associato. Il responsabile collabora nell'attuazione delle misure di sicurezza, per quanto di sua competenza, sulla base delle istruzioni ricevute dal titolare, compatibilmente con la natura e le caratteristiche del servizio fornito.

b. Il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

5.5 Dati di natura particolare

a. Nel caso in cui il trattamento effettuato tramite i servizi di hosting riguardi dati personali appartenenti a categorie particolari di cui all'art. 9 regolamento (UE) 2016/679 o dati relativi a condanne penali e reati di cui all'art. 10 regolamento (UE) 2016/679, il responsabile del trattamento, in quanto fornitore di un'infrastruttura tecnica e privo di visibilità sul contenuto dei dati trattati, mantiene una posizione di neutralità rispetto alla natura dei dati stessi e al livello di rischio ad essi associato.

b. Spetta pertanto al titolare del trattamento valutare il livello di rischio associato e indicare eventuali misure tecniche e organizzative adeguate. Su istruzione del titolare, il responsabile può adottare limitazioni specifiche e/o garanzie supplementari, compatibilmente con le caratteristiche tecniche del servizio fornito e previo accordo sul corrispettivo.

5.6. Documentazione e compliance

a. Le parti devono essere in grado di dimostrare il rispetto del presente Data Processing Agreement.

b. Il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente al presente Data Processing Agreement. Eventuali richieste di informazioni ulteriori rispetto a quelle normalmente messe a disposizione in modo standard a tutti i clienti potranno comportare l'addebito di un compenso equo, commisurato al tempo e alle risorse impiegate dal personale per fornire le risposte richieste.

c. Il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal regolamento (UE) 2016/679. Su richiesta del titolare del trattamento, il responsabile del trattamento consente e contribuisce alle attività di audit delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a una revisione o a un'attività di audit, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.

d. Il titolare del trattamento può scegliere di condurre l'attività di audit autonomamente o incaricare un auditor indipendente. Le attività di audit possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole non inferiore ai 30 giorni, in data concordata fra le parti.

Il responsabile si riserva il diritto di rifiutare l'accesso ai locali, laddove tali verifiche non risultino giustificate dalla natura, ambito, contesto e finalità del trattamento dei dati personali oggetto di audit. In particolare, potrà essere negato l'accesso o lo svolgimento dell'audit qualora:

- l'attività di verifica comporti rischi per la sicurezza fisica o informatica del soggetto auditato o dei suoi clienti;
- l'audit implichi un'interruzione significativa delle attività operative e della continuità aziendale;
- l'audit ecceda quanto strettamente necessario per la verifica della conformità alle normative applicabili.

Per questioni di sicurezza, il responsabile non consente l'accesso ai datacenter, salvo casi eccezionali e ben motivati, che richiederanno uno specifico accordo scritto fra le parti.

In ogni caso, il responsabile potrà subordinare lo svolgimento dell'audit al rimborso delle spese effettivamente sostenute, incluse quelle relative alla messa a disposizione di risorse umane e tecniche necessarie allo svolgimento dell'audit.

e. Su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di audit.

5.7 Ricorso a sub-responsabili del trattamento

a. Il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. Il responsabile del trattamento informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno 30 giorni, dando così al titolare del trattamento tempo sufficiente per potersi opporre a tali modifiche prima del ricorso al o ai sub-responsabili del trattamento in questione. Il responsabile del trattamento fornisce al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.

b. Qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento), stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente al presente Data Processing Agreement. Il responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma del presente Data Processing Agreement e del regolamento (UE) 2016/679.

c. Su richiesta del titolare del trattamento, il responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.

d. Il responsabile del trattamento rimane pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.

5.8 Trasferimenti internazionali

a. Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del regolamento (UE) 2016/679.

b. Il titolare del trattamento conviene che, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente alla clausola 5.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del regolamento (UE) 2016/679, il responsabile del trattamento e il sub-responsabile del trattamento possono garantire il rispetto del capo V del regolamento (UE) 2016/679 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

6. Assistenza al titolare del trattamento

a. Il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.

b. Il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e b), il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.

c. Oltre all'obbligo di assistere il titolare del trattamento in conformità dell'art. 6, lettera b), il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:

- l'obbligo di effettuare una valutazione d'impatto dei trattamenti previsti sulla protezione dei dati personali («Data Protection Impact Assessment») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;
- l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;
- gli obblighi di cui all'articolo 32 regolamento (UE) 2016/679.

d. Le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

e. Richieste di assistenza che eccedano quelle comrpese nei servizi contrattualizzati potranno comportare l'addebito di un compenso equo, commisurato al tempo e alle risorse impiegate dal personale per fornire le risposte richieste.

7. Notifica di una violazione dei dati personali

In caso di violazione dei dati personali («Data Breach»), il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del regolamento (UE) 2016/679, ove applicabile, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

7.1 Violazione riguardante dati trattati dal titolare del trattamento

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento assiste il titolare del trattamento:

a. nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);
b. nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del regolamento (UE) 2016/679, devono essere indicate nella notifica del titolare del trattamento e includere almeno:
    - la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
    - le probabili conseguenze della violazione dei dati personali;

- le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

c. nell'adempiere, in conformità dell'articolo 34 del regolamento (UE) 2016/679, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

7.2 Violazione riguardante dati trattati dal responsabile del trattamento

In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:

a. una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
b. i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
c. le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

Le parti stabiliscono nell'allegato III tutti gli altri elementi che il responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma degli articoli 33 e 34 del regolamento (UE) 2016/679.

SEZIONE III - DISPOSIZIONI TECNICHE

8. Diritto di accesso del cliente ai log di sistema

a. Nell'ambito dei propri obblighi di assistenza di cui alle clausole 6 e 7 del presente Data Processing Agreement, il responsabile del trattamento mette a disposizione del titolare del trattamento i dati di log alle condizioni e nei termini di cui alla seguente tabella.

	Tipo di log	Frequenza di rotazione	Accessibilità diretta del Cliente	Tempo di retention Cliente	Accessibilità su richiesta	Disponibilità
Hosting (SH, Bucket e Cloud)	Access Log del Web Server	Giornaliera	Sì	10 giorni	Sì	10 giorni
	Error Log del Web Server	Giornaliera	Sì	10 giorni	Sì	10 giorni
	Log di invio/ricezione email dai servizi di hosting (Exim)	Settimanale	Sì	Dal 1° giorno del mese in corso	Sì	30 giorni + 1
	Log di accesso caselle email dai servizi di hosting (Dovecot)	Settimanale	No	--	Sì	30 giorni +1

	Log dei rilevamenti di sicurezza (WAF-Bitninja)	Giornaliera	No	--	Sì	7 giorni
	Log FTP ai Web Server	Settimanale	No	--	Sì	4 settimane
	Log SSH ai Web Server	Giornaliera	No	--	Sì	4 settimane
	LOG back-up	Mensile	No	--	Si	1 mese

b. Le richieste di esibizione di log da parte del titolare relative a periodi antecedenti rispetto ai termini di disponibilità indicati nella suddetta tabella, saranno assoggettate ad un corrispettivo commisurato al tempo impiegato per la ricerca, nei limiti dell'importo di € 100.

c. In nessun caso il responsabile del trattamento potrà comunicare al titolare del trattamento log risalenti ad oltre un anno dalla loro generazione.

d. In qualità di fornitore di servizi di comunicazione elettronica, Host è obbligato a conservare i dati di traffico telematico, inclusi i log di sistema, anche in qualità di titolare del trattamento ed è soggetto ad obblighi di comunicazione alle pubbliche autorità, per finalità di prevenzione e repressione dei reati.

9. Metadati della posta elettronica

a. Nell'ambito della fornitura dei servizi di posta elettronica, Host potrà trattare i dati associati all'invio e alla ricezione di e-mail (c.d. dati di traffico telematico o "metadati").

I metadati della posta elettronica contengono, a titolo non esaustivo: gli indirizzi e-mail del mittente e del destinatario; gli indirizzi IP dei server o dei client coinvolti nell'instradamento del messaggio; orari di invio, di ritrasmissione o di ricezione; dimensione dei messaggi; presenza e dimensione di eventuali allegati; oggetto del messaggio.

b. Host tratta i metadati generati dai servizi di posta elettronica sia in qualità di responsabile che di titolare del trattamento, a seconda della finalità del trattamento.

In qualità di responsabile del trattamento, Host conserva i metadati per conto del Titolare (cliente) e li rende disponibili per la consultazione per un periodo massimo di 7 giorni.

In qualità di titolare del trattamento, Host tratta i medadati per finalità proprie, indipendenti dalle istruzioni del cliente. In particolare:

- per adempiere agli obblighi di legge in quanto fornitore di servizi di comunicazione elettronica, che includono la conservazione dei dati di traffico telematico per finalità di prevenzione e repressione dei reati;
- per garantire la sicurezza informatica, assicurare il corretto funzionamento dei servizi e accertare le cause di eventuali malfunzionamenti o incidenti.

Questi ultimi trattamenti sono svolti da Host in autonomia, in qualità di titolare del trattamento. Pertanto, una volta trascorso il periodo di conservazione previsto per il trattamento svolto come responsabile e salvo diverso accordo, il cliente non potrà più accedere ai metadati, poiché il loro ulteriore utilizzo è riservato esclusivamente alle finalità e alle responsabilità di Host come titolare.

SEZIONE IV - DISPOSIZIONI FINALI

10. Inosservanza delle clausole e risoluzione

a. Fatte salve le disposizioni del regolamento (UE) 2016/679, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma del presente Data Processing Agreement, il titolare del trattamento

può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti il Data Processing Agreement o non sia risolto il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare il Data Processing Agreement.

b. Il titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:

1. il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento in conformità della lettera a) e il rispetto del Data Processing Agreement non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
2. il responsabile del trattamento violi in modo sostanziale o persistente il Data Processing Agreement o gli obblighi che gli incombono a norma del regolamento (UE) 2016/679;
3. il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del regolamento (UE) 2016/679.

c. Il responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità dell'art. 5.1, lettera b), il titolare del trattamento insista sul rispetto delle istruzioni.

d. Dopo la risoluzione del contratto il responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

11. Modifiche ed aggiornamenti del Data Processing Agreement

a. Il presente Data Processing Agreement potrà essere aggiornato o modificato dal responsabile del trattamento in qualsiasi momento, al fine di:

- riflettere aggiornamenti normativi o interpretazioni giuridiche rilevanti (es. provvedimenti dell'EDPB o del Garante Privacy);
- adeguarsi a modifiche tecnologiche o organizzative nei servizi offerti;
- introdurre miglioramenti in materia di sicurezza, compliance o chiarezza contrattuale.

b. Tali modifiche saranno efficaci decorsi 30 (trenta) giorni dalla loro comunicazione al titolare del trattamento, che avverrà mediante:

- pubblicazione sul sito web ufficiale di Host e/o
- notifica via email all'indirizzo associato all'account del cliente e/o
- avviso attraverso il pannello di controllo dei servizi utilizzati.

Fatti salvi i diritti del titolare del trattamento previsti dalla normativa vigente, l'utilizzo continuato dei servizi successivamente alla scadenza del termine di 30 giorni sarà considerato accettazione tacita delle modifiche.

Nel caso in cui il titolare del trattamento ritenga che le modifiche comportino un pregiudizio sostanziale ai propri diritti o obblighi in materia di protezione dei dati, potrà comunicare per iscritto la propria opposizione entro il termine di cui sopra. In tale ipotesi, le parti si confronteranno in buona fede per individuare una soluzione contrattuale alternativa. Resta salva la facoltà del titolare del trattamento di cessare il rapporto contrattuale secondo i termini e le condizioni generali di servizio applicabili.

ALLEGATO I

Parti del Data Processing Agreement

Responsabile/i del trattamento

Responsabile del trattamento è la società Host S.p.a., con sede in Corso Svizzera 185, 10149 Torino (TO), in persona del suo legale rappresentante Marco Mangione, contattabile ai seguenti recapiti:

E-mail info@host.it

PEC info@pec.host.it

Tel. 800 943 944

Responsabile della Protezione dei Dati

Il Responsabile della Protezione dei Dati (RPD) di Host S.p.a. è l'Avv. Massimo Bacci, contattabile ai seguenti recapiti:

E-mail privacy@host.it

Tel. +39 0574 870551

Titolare del trattamento

Titolare del trattamento è il cliente che ha acquistato da Host S.p.a. servizi che comportano trattamenti di dati personali da parte di quest'ultima, i cui dati sono specificati nel contratto di servizi di cui il presente Data Processing Agreement costituisce un Addendum.

ALLEGATO II

Descrizione del trattamento

Il responsabile tratta, per conto del titolare del trattamento, dati personali nell'ambito dell'erogazione dei propri servizi di Cloud Computing, inclusi servizi di hosting, gestione di domini, posta elettronica, PEC, sicurezza web, backup e supporto tecnico.

Tali trattamenti possono consistere nella conservazione, trasmissione, organizzazione, cancellazione, pseudonimizzazione, cifratura e, in alcuni casi, accesso ai dati personali presenti sulle infrastrutture tecniche messe a disposizione dal responsabile.

Il trattamento avviene esclusivamente secondo le istruzioni del titolare del trattamento e nei limiti delle funzionalità tecniche del servizio attivato.

Categorie di interessati i cui dati personali sono trattati

Le categorie di interessati i cui dati personali possono essere trattati, in funzione del servizio attivato dal titolare del trattamento, possono includere:

- Clienti e potenziali clienti del titolare del trattamento;
- Dipendenti, collaboratori, consulenti del titolare del trattamento;
- Utenti finali dei servizi erogati dal titolare del trattamento;
- Fornitori, partner commerciali o altri soggetti in rapporto con il titolare del trattamento;
- Mittenti e destinatari delle comunicazioni elettroniche gestite tramite i servizi del responsabile del trattamento;
- Altre persone fisiche i cui dati sono trattati dal titolare utilizzando i servizi o le infrastrutture forniti dal responsabile del trattamento.

Categorie di dati personali trattati

I dati personali oggetto di trattamento possono includere:

- Dati anagrafici e identificativi;
- Dati di contatto (email, PEC, numero di telefono);
- Dati tecnici (indirizzi IP, log di accesso, dati di utilizzo dei servizi, dati di configurazione, metadati della posta elettronica);

- Dati contenuti in file, database, caselle email e altri archivi memorizzati dal titolare del trattamento nelle infrastrutture di hosting;
- Dati relativi alla navigazione, se inclusi nei log web;
- Categorie particolari di dati (ex artt. 9 e 10 GDPR) solo se il titolare del trattamento ne prevede il trattamento nei propri contenuti, sotto la sua esclusiva responsabilità;
- Altri dati personali trattati dal titolare del trattamento utilizzando i servizi o le infrastrutture forniti dal responsabile del trattamento.

Natura del trattamento

Il trattamento ha natura prevalentemente automatizzata e consiste nella messa a disposizione di infrastrutture IT, nella conservazione e gestione tecnica dei dati, nella loro trasmissione su richiesta, nonché nella protezione da accessi non autorizzati.

Il responsabile del trattamento non accede ai dati per finalità proprie e adotta una posizione di neutralità rispetto al contenuto dei dati trattati, fatti salvi gli obblighi di assistenza e cooperazione con il titolare del trattamento o le Autorità competenti.

Finalità per le quali i dati personali sono trattati per conto del titolare del trattamento

I dati personali sono trattati esclusivamente per:

- Consentire l'erogazione dei servizi acquistati dal titolare del trattamento (hosting, email, backup, gestione domini, etc.);
- Garantire il corretto funzionamento e la disponibilità dell'infrastruttura;
- Fornire assistenza tecnica al titolare del trattamento;
- Supportare il titolare del trattamento in caso di violazioni di dati personali o altri eventi critici;
- Adempiere a eventuali obblighi derivanti da richieste legittime del titolare del trattamento o delle Autorità competenti.

Durata del trattamento

I dati personali saranno trattati per tutta la durata del rapporto contrattuale tra Host e il titolare del trattamento.

Alla cessazione del contratto, i dati saranno cancellati o restituiti al titolare del trattamento secondo quanto previsto dall'accordo, salvo eventuali obblighi di legge che impongono la loro ulteriore conservazione da parte del responsabile del trattamento.

Eventuali log e metadati tecnici potranno essere conservati da Host per periodi più lunghi, in conformità alla normativa applicabile e alla documentazione tecnica, ma non saranno più accessibili al titolare del trattamento salvo diversa previsione contrattuale.

ALLEGATO III

Descrizione delle misure di sicurezza

Il responsabile si impegna a garantire un livello di sicurezza non inferiore a quanto previsto dalle misure tecniche ed organizzative descritte di seguito.

1. Procedure sulla sicurezza dei dati

Sono stati definiti ruoli e responsabilità separati per la sicurezza dei dati e sono stati assegnati ai dipendenti ed ai collaboratori autorizzati al trattamenti dei dati personali della Società (di seguito anche "utenti") per evitare conflitti di interesse e prevenire attività inappropriate ed abusi.

2. Sicurezza delle risorse umane

È previsto un regolamento sulla sicurezza per l'utilizzo di tutti i dispositivi aziendali assegnati agli utenti.

Al momento dell'uscita di un utente da Host, o nel caso di modifica significativa del ruolo assegnato, i permessi di accesso vengono aggiornati immediatamente, gli strumenti e gli accessi ai servizi aziendali riconfigurati.

3. Gestione dei beni di proprietà aziendale

Tutti i beni del patrimonio aziendale sono accuratamente inventariati ed è monitorata l'assegnazione delle stesse ai vari utenti che sono responsabili per la loro sicurezza. È definito un regolamento per l'uso corretto dei beni.

4. Controllo degli accessi ai sistemi

I requisiti organizzativi aziendali per il controllo degli accessi alle risorse informative sono documentati in una procedura con le relative misure di sicurezza. L'accesso alla rete ed alle connessioni è protetto da firewall e sistemi di sicurezza di nuova generazione.

L'assegnazione dei diritti e privilegi di accesso agli utenti è regolamentata, a partire dalla registrazione iniziale dell'utente fino alla rimozione dei diritti di accesso, quando non più necessari, incluse le speciali restrizioni per i diritti di accesso privilegiato e la gestione delle "informazioni segrete di autenticazione". Nella gestione degli accessi viene utilizzato il criterio del "minimo privilegio", i diritti di accesso sono forniti in modo da permettere all'utente l'accesso ai soli dati necessari per la sua attività. Diritti di accesso ulteriori richiedono una specifica autorizzazione.

Gli utenti sono informati sulle loro responsabilità anche attraverso il mantenimento di un effettivo controllo degli accessi e mantenendoli riservati.

L'accesso alle informazioni è soggetto a restrizioni nel rispetto della politica sul controllo degli accessi, attraverso un sistema di accessi sicuri, di gestione delle password e delle loro scadenze, del controllo sulle utilità privilegiate e l'accesso limitato a tutti i codici sorgente.

5. Cifratura

È presente un regolamento interno sull'uso della cifratura dei dispositivi degli utenti. Le autenticazioni sono criptate.

6. Sicurezza fisica e perimetrale

I servizi offerti dalla Società vengono erogati attraverso data center qualificati, di proprietà diretta o con cui vige un contratto di fornitura. Tutti i data center utilizzati dispongono di ridondanza completa di tutti i circuiti elettrici, di raffreddamento e di rete.

L'accesso fisico ai data center è regolato e controllato da procedure di autorizzazione, riconoscimento e registrazione degli accessi ed è limitato ai soli operatori autorizzati.

È attivo sui dispositivi aziendali il controllo dei virus e dei malware e c'è un'idonea consapevolezza sui rischi informatici da parte degli utenti.

Nel servizio email il traffico di posta viene analizzato in tempo reale, sia in ingresso che in uscita, per il rilevamento di virus, malware e per l'identificazione e il filtraggio dello spam e del phishing.

L'analisi è automatica e si basa sia sulla natura del contenuto, sia sull'interrogazione di basi dati internazionali, sia sulla reputazione acquisita grazie a una serie di parametri.

Vengono eseguiti backup periodici, ad esclusione dei servizi per i quali è responsabilità del cliente effettuare e gestire i backup. Ulteriori backup, non accessibili dai clienti, vengono effettuati a solo scopo di Disaster Recovery.

L'accesso ai sistemi interni è consentito esclusivamente da reti autorizzate e VPN aziendali.

7. Autenticazione e monitoraggio

Ogni attività ed evento relativo alla sicurezza delle informazioni da parte degli utenti del sistema e degli amministratori ed operatori avviene previo inserimento delle credenziali di autenticazione. Gli orologi di tutte le apparecchiature sono sincronizzati.

L'installazione di software sui sistemi operativi degli utenti è controllata e monitorata tramite un apposito software e consultabile in maniera centralizzata.

8. Gestione delle vulnerabilità tecniche

Ogni vulnerabilità tecnica a noi nota viene corretta con adeguate patch non appena disponibili dal fornitore del software. Sono previste procedure per le fasi di test e per la conseguente installazione degli aggiornamenti che avviene solo quando tutti i test hanno avuto esito positivo.

9. Rapporti con i fornitori

Sono previsti contratti o accordi volti a proteggere e a disciplinare il trattamento delle informazioni dell'organizzazione e dei clienti nel caso in cui siano accessibili a soggetti terzi o ad altri fornitori presenti nell'intera catena di fornitura.

10. Gestione degli incidenti relativi alla sicurezza delle informazioni

Sono previste responsabilità e procedure apposite volte a gestire in modo coerente ed efficace gli eventi e gli eventuali incidenti relativi alla sicurezza delle informazioni (ad es. procedura di Data Breach).

11. Sicurezza delle informazioni e continuità aziendale

Tutte le principali strutture informatiche in uso sono ridondate per soddisfare i requisiti di disponibilità. Laddove questa ridondanza non è in essere, sono in atto adeguate misure per garantire la continuità del servizio o la riduzione al minimo della perdita di dati.

ALLEGATO IV

Elenco dei sub-responsabili del trattamento

DENOMINAZIONE	DESCRIZIONE DEI SERVIZI
Aruba PEC S.p.a.	Fornitore servizi PEC.
BitNinja Technologies ZMR	Sistema di sicurezza. Traccia gli indirizzi IP degli utenti in caso di incidenti di sicurezza.
Fastnetmon Ltd	Servizio di monitoraggio sicurezza per prevenzione DDoS Attacks.
Halon Security AB	Provider sistema di filtraggio e-mail (antispam).
Infocert S.p.a.	Fornitore servizi PEC.
Vianova S.p.a.	Fornitura Datacenter per alcuni servizi di hosting verso clienti, infrastruttura di back-up e nodi posta elettronica.
Seltium di Stefano Cau	Servizi di montaggio server e manutenzione dell'infrastruttura reti.
Open Technologies di Martra Andrea e C. S.a.s.	Servizi di consulenza informatica su VPS e applicativi OpenStack.
Daimonet di Pascal Abatiello	Gestione e sviluppo della Business Unit Host Academy tramite creazione di materiale formativo e supervisione delle attività.
Andrea Sacca Consulting S.L.U.	Servizi di gestione, supervisione e sviluppo dei rapporti con i clienti.
NetResult S.r.l.	Fornitura e servizio di supporto e assistenza Kalliope Public Cloud.
Impresa individuale Landolina Ruggero	Servizi di sviluppo, manutenzione e assistenza su siti web Magento.