ALLEGATO F — ACCEPTABLE USE POLICY (AUP)

Ultima modifica: 22/09/2026 | Versione: AUP-2026-09-22

TimeFlow S.r.l. SB — documento contrattuale del Trust Center

Da sapere a colpo d'occhio

- Uso delle Piattaforme riservato agli Utenti Autorizzati, per sole finalità interne della Committente e nei limiti dell'Ordine.
- Vietati, tra l'altro, scraping e crawling, reverse engineering, test di sicurezza non autorizzati e immissione di categorie particolari di dati.
- Enforcement graduale e proporzionato, dall'avviso alla sospensione; i disservizi riconducibili a violazioni della AUP sono esclusi dal calcolo SLA.

Definizioni

Ai fini del presente Allegato, i seguenti termini, ove utilizzati con lettera iniziale maiuscola, hanno il significato di seguito indicato. Per i termini non qui definiti, si rinvia alle Definizioni del MSA (Allegato A).

- **AUP (Acceptable Use Policy):** indica il presente documento, che disciplina le regole di uso consentito e vietato delle Piattaforme e dei Servizi.
- **Benchmarking Pubblico:** indica la pubblicazione o la comunicazione a terzi di risultati di test comparativi eseguiti sulle Piattaforme senza il preventivo consenso scritto del Fornitore.
- **Burst (API):** indica un picco temporaneo di richieste API eccedente il rate medio consentito; il Burst può essere ammesso entro le soglie documentate nella documentazione tecnica.
- **Crawling/Scraping:** indica qualsiasi automazione che estragga o navighi sistematicamente contenuti o interfacce delle Piattaforme, aggirando le modalità di utilizzo ordinario.
- **Decompilazione:** indica la ricostruzione del codice sorgente a partire dal codice eseguibile, dal bytecode o da qualsiasi forma intermedia del software.
- **DoS/DDoS:** indica gli attacchi, singoli o distribuiti, volti a rendere indisponibili i Servizi mediante la saturazione intenzionale delle risorse computazionali, di rete o di storage.
- **Duty to Mitigate:** indica l'obbligo reciproco delle Parti di cooperare attivamente per ridurre e contenere gli impatti di un disservizio o di una violazione contrattuale (cfr. MSA §12.8).

- **Enforcement:** indica l'insieme delle misure applicative che TimeFlow può adottare in caso di violazione della presente AUP, graduate secondo il principio di proporzionalità (avvisi, limitazioni, sospensioni, risoluzione).
- **Export Control / Sanzioni:** indica le normative che vietano o limitano l'utilizzo dei Servizi da parte di o verso soggetti, entità o Paesi sottoposti a sanzioni internazionali o a restrizioni all'esportazione.
- **Fair Use (API):** indica l'utilizzo delle API conforme ai limiti quantitativi, alle finalità e ai carichi ragionevoli indicati nella documentazione tecnica e nel Contratto.
- **Malware:** indica qualsiasi software, codice o script malevolo progettato per danneggiare, alterare, interrompere o compromettere il funzionamento di sistemi, reti o dati.
- **MFA (Multi-Factor Authentication):** indica il metodo di autenticazione basato sulla verifica di almeno due fattori indipendenti (a titolo esemplificativo: password e codice OTP).
- **PCI DSS:** indica il Payment Card Industry Data Security Standard; l'utilizzo delle Piattaforme per il trattamento di dati soggetti a PCI DSS richiede la sottoscrizione di specifici accordi e l'adozione di misure dedicate.
- **Phishing/Spam:** indica l'invio di messaggi ingannevoli (phishing) o di comunicazioni massive non sollecitate (spam) attraverso i canali integrati nelle Piattaforme (e-mail, SMS).
- **Rate Limit:** indica la soglia massima di richieste per unità di tempo applicata alle API e ai Servizi, come documentata nella specifica tecnica.
- **Reverse Engineering:** indica qualsiasi analisi tecnica finalizzata a ricostruire il funzionamento interno, la logica, gli algoritmi o l'architettura dell'applicazione o dei suoi componenti.
- **RPA (Robotic Process Automation):** indica il software che emula le azioni di un utente su interfacce UI o API; il suo utilizzo è consentito esclusivamente in conformità alle licenze e ai limiti d'uso contrattuali.
- **Scope (API):** indica l'insieme dei permessi assegnati a un token o a una chiave API, che delimita le operazioni consentite al titolare della credenziale.
- **Service Bureau:** indica l'utilizzo delle Piattaforme o dei Servizi per erogare, direttamente o indirettamente, a soggetti terzi diversi dagli Utenti Autorizzati, servizi equivalenti o funzionalmente analoghi in conto terzi.
- **Stress/Load Test:** indica i test che generano carichi elevati sulle Piattaforme ovvero le scansioni di sicurezza; tali attività sono ammesse esclusivamente previa autorizzazione scritta di TimeFlow e all'interno di finestre temporali concordate.
- **Takedown:** indica la rimozione o la disabilitazione, da parte di TimeFlow, di contenuti immessi nella Piattaforma che risultino illeciti, lesivi di diritti di terzi o in violazione della normativa applicabile.
- **Throttling:** indica la limitazione dinamica e temporanea del volume delle richieste, adottata da TimeFlow per proteggere la stabilità e la sicurezza dei Servizi.

- **Token / API Key:** indica la credenziale tecnica emessa da TimeFlow per l'autenticazione delle chiamate API, soggetta a rotazione periodica e ai relativi Scope.
- **Utenti Autorizzati:** indica le persone fisiche identificate dalla Committente e legittimate all'accesso alle Piattaforme secondo i profili, i ruoli e i limiti d'uso tempo per tempo vigenti, come definito nel MSA.

1. Scopo e ambito di applicazione

1.1 Finalità. La presente Acceptable Use Policy ("AUP") definisce le regole di utilizzo consentito e vietato delle Piattaforme TimeFlow, come definite nel MSA e individuate dai relativi Addenda di Prodotto (alla data della presente versione, WMP, VMP e TimeFlow Source), e dei relativi Servizi erogati da TimeFlow.

1.2 Coordinamento contrattuale. La presente AUP si coordina con il MSA (in particolare §§ 2, 7, 8, 9, 14, 15, 17 e 18), con lo SLA – Allegato C (con specifico riferimento a: §2 Misurazione, §3 Target e crediti, §4 Claim, §5 Manutenzioni, §6 Esclusioni, §7 Gestione incidenti) e con l'Allegato D (TOMs & BC/DR). In caso di conflitto, si applica l'ordine di prevalenza stabilito nel MSA §18.5.

2. Usi consentiti e responsabilità della Committente

2.1 Soggetti legittimati. L'accesso alle Piattaforme è riservato agli Utenti Autorizzati e agli eventuali Account Tecnici previsti nell'Ordine o nella documentazione tecnica applicabile (cfr. MSA §2.2 e Definizioni). Le credenziali di accesso sono strettamente personali e non condivisibili (cfr. MSA §7).

2.2 Finalità lecite e interne. L'utilizzo delle Piattaforme e dei Servizi è consentito esclusivamente per le finalità di business interne della Committente, nei limiti quantitativi e qualitativi stabiliti nell'Ordine (utenze, profili/record, moduli, ambienti) e nel rispetto della normativa applicabile (cfr. MSA §§ 2.1–2.4 e 7).

2.3 Requisiti tecnici e identity management. La Committente è tenuta a mantenere aggiornati i browser e gli endpoint supportati e, ove il Single Sign-On sia abilitato, a gestire correttamente il proprio Identity Provider (cfr. MSA §3.2 e §4.4).

2.4 Diligenza nella gestione degli accessi. La Committente provvede tempestivamente al provisioning e al de-provisioning degli Utenti Autorizzati, abilita l'autenticazione multifattore ove prevista, custodisce le credenziali e le chiavi API con la diligenza richiesta dalla natura del Servizio e notifica tempestivamente a TimeFlow qualsiasi abuso, accesso non autorizzato o sospetto di compromissione (cfr. MSA §7).

3. Usi vietati

Fermo restando quanto previsto dal MSA §2.5 (Divieti), sono espressamente vietati i seguenti comportamenti e attività:

(a) Attività illecite e abusi. Lo svolgimento di attività contrarie alla legge, la commissione di frodi, l'invio di spam o phishing, l'invio massivo non sollecitato attraverso i canali e-mail o SMS integrati nelle Piattaforme, l'elusione o l'aggiramento dei controlli tecnici predisposti da TimeFlow, nonché l'utilizzo delle Piattaforme in violazione delle normative applicabili in materia di sanzioni internazionali e controllo all'esportazione (cfr. MSA §2.9 e §7).

(b) Violazioni della sicurezza. L'introduzione di malware, exploit, virus o codice malevolo; i tentativi di intrusione o di accesso non autorizzato ai sistemi; l'esecuzione di test di sicurezza, vulnerability scan o penetration test senza il preventivo consenso scritto di TimeFlow e al di fuori delle finestre temporali e del perimetro concordati (cfr. MSA §2.5 e Allegato D §3).

(c) Automazioni non consentite. Le attività di scraping e crawling; l'utilizzo di software RPA o di bot che simulino il comportamento di utenti al fine di eludere le licenze, i Rate Limit o i limiti di Burst; l'esecuzione di stress test o load test non preventivamente concordati per iscritto (cfr. MSA §§ 2.4–2.5, Allegato D §3.5).

(d) Saturazione delle risorse e alterazione della stabilità. Qualsiasi attività volta a saturare intenzionalmente le risorse computazionali, di rete o di storage (a titolo esemplificativo: mining di criptovalute, attacchi DoS/DDoS), nonché qualsiasi tentativo di eludere i meccanismi di throttling predisposti dal Fornitore (cfr. MSA §2.4, SLA §6).

(e) Violazioni della proprietà intellettuale e benchmarking. Il reverse engineering e la decompilazione delle Piattaforme; il benchmarking pubblico non autorizzato per iscritto; il sublicenziamento; l'utilizzo in modalità service bureau; la messa a disposizione delle Piattaforme a soggetti diversi dagli Utenti Autorizzati (cfr. MSA §2.5 e §15).

(f) Dati e contenuti vietati. L'immissione nelle Piattaforme di dati appartenenti a categorie particolari ai sensi dell'art. 9 del GDPR o di dati giudiziari ai sensi dell'art. 10 del GDPR, salva espressa deroga scritta tra le Parti (cfr. MSA §8.9 e, per ciascuna Piattaforma, il DPA ovvero l'informativa privacy applicabile secondo il relativo Addendum di Prodotto). È altresì vietata l'immissione di contenuti illeciti o lesivi di diritti di terzi.

(g) Dati reali in ambienti non produttivi. L'utilizzo di dati reali della Committente negli ambienti sandbox o UAT, salvo diverso accordo scritto tra le Parti con adozione delle misure di sicurezza dedicate previste dal MSA §2.8 e dall'Allegato D §2.6.

(h) Usi vietati specifici di TimeFlow Source. L'utilizzo dei Dati di Contatto Nominativi e delle funzioni RFI per comunicazioni promozionali, per finalità estranee allo scouting e alla qualifica di fornitori per conto della Committente o in violazione delle richieste dei referenti di non essere ricontattati; l'estrazione massiva, il riutilizzo al di fuori del tenant e la rivendita dei dati della Base Dati Societaria Condivisa e delle fonti terze rese disponibili dalla piattaforma; l'immissione di dati personali nella Base Dati Societaria Condivisa; l'attivazione o l'utilizzo dell'Add-on Arricchimento Contatti in difformità

dall'Addendum di Prodotto TimeFlow Source, Art. 6. I termini con iniziale maiuscola hanno il significato loro attribuito dal medesimo Addendum.

4. API, integrazioni e fair use

4.1 Credenziali e scope. L'utilizzo delle API richiede l'impiego di chiavi e token di autenticazione rilasciati da TimeFlow e il rispetto degli Scope assegnati e della documentazione tecnica applicabile.

4.2 Rate Limit e Burst. Si applicano i Rate Limit e, ove previsto, le soglie di Burst documentati nella specifica tecnica. In caso di superamenti non occasionali, TimeFlow potrà adottare misure di Throttling ovvero blocchi mirati degli endpoint impattati, in conformità a quanto previsto dal MSA §2.4 e dall'Allegato D §3.5.

4.3 Test di carico e scansioni. L'esecuzione di stress test, load test, scansioni di vulnerabilità o qualsiasi altra attività suscettibile di impattare la disponibilità o la sicurezza dei Servizi è consentita esclusivamente previa autorizzazione scritta di TimeFlow, con definizione del perimetro e della finestra temporale (cfr. MSA §2.5, SLA §5).

4.4 Integrazioni con sistemi terzi. Le integrazioni verso sistemi e servizi della Committente richiedono che quest'ultima disponga delle corrette licenze e quote e che adotti le idonee misure di sicurezza. Eventuali disservizi riconducibili a tali integrazioni rientrano nelle Esclusioni dello SLA (cfr. SLA §6).

5. Dati e contenuti

5.1 Liceità e minimizzazione. La Committente garantisce la sussistenza delle basi giuridiche per il trattamento e la liceità dei dati immessi nelle Piattaforme, adottando i principi di minimizzazione previsti dalla normativa applicabile. La Committente è e resta l'unica responsabile della sicurezza e della retention degli export e delle copie locali dei dati estratti dalle Piattaforme (cfr. MSA §§ 7 e 8). Con riferimento a TimeFlow Source, la Committente, quale titolare, provvede a rendere l'informativa ai referenti delle aziende target ai sensi dell'art. 14 del GDPR, anche avvalendosi del modello messo a disposizione da TimeFlow (Appendice 2 al DPA, Art. 8).

5.2 Categorie di dati vietate o soggette a restrizione. È vietata l'immissione nelle Piattaforme di dati appartenenti a categorie particolari o giudiziarie ai sensi degli artt. 9 e 10 del GDPR, salva espressa deroga scritta tra le Parti. È altresì vietato il caricamento di dati soggetti a standard settoriali specifici (a titolo esemplificativo: PCI-DSS, dati sanitari regolamentati) in assenza di apposito accordo scritto e di misure di sicurezza dedicate (cfr. MSA §8.9).

5.3 Takedown. TimeFlow si riserva la facoltà di rimuovere o disabilitare, senza preavviso ove giustificato dall'urgenza, i contenuti immessi nelle Piattaforme che risultino illeciti, lesivi di diritti di terzi o in violazione della normativa applicabile, ai sensi del MSA e della legge.

6. Monitoraggio, enforcement e rimedi

6.1 Metriche e log. TimeFlow è autorizzata a raccogliere e analizzare metriche d'utilizzo e log per finalità di erogazione del Servizio, sicurezza, miglioramento continuo e verifica della conformità ai limiti d'uso contrattuali (cfr. MSA §2.6, Allegato D §2.5).

6.2 Escalation e misure proporzionate. In caso di violazioni della presente AUP o di rischi per l'integrità e la sicurezza dei sistemi, TimeFlow adotterà le seguenti misure, graduate secondo il principio di proporzionalità: (i) avviso scritto alla Committente e richiesta di correzione entro un termine ragionevole; (ii) Throttling o limitazioni mirate degli endpoint o delle funzionalità impattate; (iii) sospensione parziale o totale dell'accesso alle Piattaforme ai sensi del MSA §§ 2.7 e 14.1; (iv) ove la violazione integri un grave inadempimento, risoluzione del Contratto ai sensi del MSA §6.5.

6.3 Impatto sullo SLA e sui Service Credits. I tempi di indisponibilità e gli impatti riconducibili a violazioni della presente AUP da parte della Committente rientrano nelle Esclusioni dello SLA (cfr. SLA §6) e non conferiscono diritto al riconoscimento di Service Credits (cfr. SLA §§ 3–4). Durante le sospensioni, TimeFlow potrà consentire alla Committente l'accesso in sola lettura e/o l'export limitato dei dati, ove tecnicamente compatibile con la natura della sospensione (cfr. MSA §2.7).

6.4 Obbligo di mitigazione. Le Parti cooperano in buona fede per mitigare gli impatti delle violazioni e ripristinare la conformità nel più breve tempo possibile (cfr. MSA §12.8).

7. Segnalazioni, canali e aggiornamenti

7.1 Segnalazioni di abusi o vulnerabilità. La Committente è tenuta a segnalare tempestivamente a TimeFlow qualsiasi abuso, incidente di sicurezza o vulnerabilità rilevata, tramite i canali operativi indicati nell'Ordine e richiamati nello SLA §9. Gli eventuali incidenti che coinvolgano Dati Personali sono soggetti alla procedura di notifica prevista dal MSA §8.5 (notifica senza ingiustificato ritardo ed entro settantadue ore dalla conoscenza).

7.2 Aggiornamenti della AUP. Gli aggiornamenti del presente Allegato sono disciplinati dal MSA §18.3. Nessun aggiornamento produce effetti retroattivi su fatti già avvenuti.

7.3 Sopravvivenza. Le clausole della presente AUP relative a enforcement, responsabilità, comunicazioni e ordine di prevalenza sopravvivono alla cessazione del Contratto nei limiti necessari alla tutela dei diritti delle Parti (cfr. MSA §§ 12, 13, 17–19).

8. Disposizioni finali

Per l'ordine di prevalenza tra i documenti contrattuali e per le modalità di aggiornamento del presente Allegato si applica il MSA, §§18.3 e 18.5. Le violazioni della presente AUP possono attivare le misure di sospensione previste dal MSA §§ 2.7 e 14.1.