ALLEGATO K — API & PERSONALIZZAZIONI

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

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

Da sapere a colpo d'occhio

- API REST documentate in OpenAPI, webhooks con firma HMAC, connettori e personalizzazioni gestiti su progetto con Piano di Integrazione.
- Versioning semantico con retrocompatibilità garantita per release minor e patch; breaking change solo in occasione di nuove major version.
- Variazioni di perimetro gestite tramite Change Request formali; API e connettori erogati da TimeFlow rientrano nel perimetro dello 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).

- **Backoff Esponenziale:** indica la strategia di retry che incrementa progressivamente l'intervallo temporale tra i tentativi successivi (a titolo esemplificativo: 1s, 2s, 4s, 8s), al fine di ridurre la pressione sul sistema ricevente in caso di errore temporaneo.
- **Breaking Change:** indica una modifica incompatibile con i client esistenti (a titolo esemplificativo: rimozione o modifica della semantica di campi o endpoint), introdotta esclusivamente in occasione di una nuova major version.
- **Changelog:** indica il registro strutturato delle modifiche rilasciate, comprensivo di nuove funzionalità, correzioni, deprecazioni e variazioni di schema o endpoint.
- **Dead-Letter Queue (DLQ):** indica la coda di destinazione dei messaggi o eventi non consegnabili dopo l'esaurimento dei tentativi di retry, ai fini dell'analisi e dell'eventuale ri-processamento.
- **Firma HMAC:** indica la firma del payload effettuata mediante chiave condivisa secondo lo standard Hash-based Message Authentication Code (HMAC), al fine di garantire l'integrità e l'autenticità delle notifiche (in particolare: webhooks).
- **Hypercare:** indica la finestra di assistenza tecnica rafforzata immediatamente successiva al go-live, focalizzata sulla stabilizzazione del sistema e sul tuning delle configurazioni.
- **Idempotenza:** indica la proprietà per la quale la ripetizione della medesima richiesta produce invariabilmente il medesimo risultato, evitando duplicazioni in caso di retry.

- **iPaaS/ESB:** indica le piattaforme di integrazione (Integration-Platform-as-a-Service) e gli Enterprise Service Bus utilizzati per orchestrare, trasformare e instradare i flussi di dati tra sistemi eterogenei.
- **mTLS (mutual TLS):** indica il protocollo di autenticazione reciproca (client e server) mediante certificati digitali, nell'ambito di una connessione TLS.
- **Near-Real-Time (NRT):** indica la modalità di scambio dati con latenza ridotta ma non istantanea (dell'ordine di secondi o minuti), tipicamente implementata tramite webhooks o code di messaggi.
- **OpenAPI/Swagger:** indica la specifica e il relativo set di strumenti per la descrizione formale delle API REST (endpoint, metodi HTTP, schemi di richiesta/risposta, esempi), utilizzata per la generazione automatica di client e documentazione.
- **Payload:** indica il contenuto informativo della richiesta o della risposta (tipicamente in formato JSON) trasmesso da o verso un'API ovvero contenuto in un evento.
- **Piano di Integrazione:** indica il documento progettuale che definisce il perimetro dei flussi, le mappature dei campi, i requisiti di sicurezza, i KPI, i volumi stimati, le finestre operative e la ripartizione delle responsabilità tra le Parti.
- **Retry:** indica il ritentativo automatico di consegna o esecuzione effettuato a seguito di un errore temporaneo, tipicamente con strategia di Backoff Esponenziale e con un numero massimo di tentativi predefinito.
- **SCIM:** indica lo standard System for Cross-domain Identity Management, utilizzato per il provisioning e il de-provisioning automatizzato di utenti e gruppi tra sistemi di gestione delle identità.
- **SFTP / S3-compatibile:** indica i protocolli e i servizi per il trasferimento e il deposito sicuro di file; SFTP utilizza il protocollo SSH, mentre i servizi S3-compatibili espongono API conformi allo standard Amazon S3 per la gestione di oggetti.
- **Versioning Semantico (SemVer):** indica lo schema di versionamento MAJOR.MINOR.PATCH; la compatibilità con le versioni precedenti è garantita per le release minor e patch, mentre le modifiche incompatibili (Breaking Change) sono introdotte esclusivamente nelle release major, con periodo di coesistenza e deprecazione.

1. Scopo e ambito di applicazione

Il presente Allegato disciplina le integrazioni, l'utilizzo delle API, i webhooks e gli eventi, le personalizzazioni applicative e i connettori relativi alle Piattaforme TimeFlow, come definite nel MSA e individuate dai relativi Addenda di Prodotto (alla data della presente versione, WMP, VMP e TimeFlow Source), ivi inclusi il perimetro delle attività, i deliverable, la governance tecnica e gli oneri economici. Le disposizioni del presente Allegato si applicano salva diversa ed espressa pattuizione nell'Ordine o nella SOW.

2. Oggetto

2.1 API. Interfacce di programmazione esposte secondo il paradigma REST/JSON su protocollo HTTPS.

2.2 Webhook/Eventi. Notifiche push server-to-server trasmesse verso endpoint della Committente al verificarsi di eventi predefiniti.

2.3 Connettore. Componente software, in modalità batch o Near-Real-Time, che realizza l'integrazione con applicazioni di terze parti.

2.4 Personalizzazione. Estensioni funzionali o configurazioni avanzate che eccedono il perimetro delle funzionalità standard delle Piattaforme.

3. Catalogo API e modelli dati

Le API REST sono documentate in formato OpenAPI e coprono, a titolo esemplificativo e non esaustivo, i seguenti domini funzionali: projects, company, users, jobSector, services, technology, languages, certifications (con operazioni CRUD ove applicabili). L'elenco puntuale degli endpoint e i relativi schemi di richiesta/risposta sono pubblicati nel tenant della Committente e nel documento "TimeFlow – API List". Gli endpoint possono essere soggetti ad evoluzione; la loro disponibilità attuale non costituisce impegno del Fornitore a esporre ogni operazione su tutti i tenant.

4. Webhooks ed eventi

4.1 Attivazione. I webhooks sono attivabili su richiesta della Committente per specifiche tipologie di eventi (a titolo esemplificativo: operazioni CRUD su progetti, esigenze, profili/risorse, candidature, utenti, stati di trattativa).

4.2 Sicurezza. Le notifiche webhook possono essere protette mediante firma HMAC (opzionale), IP allowlist e/o mTLS, su richiesta della Committente.

4.3 Affidabilità. TimeFlow implementa meccanismi di retry con Backoff Esponenziale. Una Dead-Letter Queue (DLQ) è attivabile su richiesta per la gestione dei messaggi non consegnabili.

4.4 Specifiche tecniche. I dettagli relativi a payload, headers, tempi di consegna e formati sono definiti nel Piano di Integrazione.

5. Sicurezza e controlli di accesso

5.1 Autenticazione. L'accesso alle API avviene mediante bearer token. Su richiesta della Committente, è disponibile l'autenticazione tramite OAuth2/OIDC con l'Identity Provider della Committente (protocolli SAML 2.0 o OIDC) per i flussi server-to-server; per le integrazioni puramente tecniche si utilizzano API key dedicate.

5.2 Autorizzazione. L'accesso è governato da un modello di scoping granulare basato su tenant, ruoli e permessi, in applicazione del principio del minimo privilegio (Least Privilege).

5.3 Hardening e logging. Tutte le chiamate API sono soggette ad audit trail e logging applicativo. I dati di telemetria sono disponibili per finalità di troubleshooting e monitoraggio dei KPI di integrazione.

5.4 Rate limiting e throttling. Sono applicati limiti di richieste per client e per tenant, con controllo del burst. In caso di superamenti non occasionali, TimeFlow potrà applicare Throttling ovvero sospensione mirata dei soli endpoint impattati, in conformità a quanto previsto dal MSA §2.4 e dall'AUP (Allegato F).

5.5 Misure aggiuntive. Su richiesta della Committente sono disponibili: IP allowlist e mTLS. Per il dettaglio delle ulteriori misure di sicurezza si rinvia all'Allegato D (TOMs & BC/DR).

6. Ambienti, versioning e compatibilità

6.1 Ambienti. L'ambiente di produzione è localizzato in territorio UE/SEE. Ambienti di test o staging sono disponibili su richiesta; non è consentito l'utilizzo di dati reali della Committente in tali ambienti, 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.

6.2 Versioning delle API. Le API adottano il Versioning Semantico (SemVer), con identificazione della versione nel path (vN).

6.3 Compatibilità. La retrocompatibilità è garantita per le release minor e patch. I Breaking Change sono introdotti esclusivamente in occasione di nuove major version.

6.4 Deprecazioni. Le deprecazioni di endpoint o funzionalità sono comunicate con preavviso adeguato. TimeFlow garantisce la coesistenza delle versioni major per un periodo proporzionato all'impatto della transizione. Il processo di change management e i relativi preavvisi si coordinano con il MSA §9.5 e con lo SLA – Allegato C §5.

7. Modelli di integrazione supportati

TimeFlow supporta i seguenti modelli di integrazione, selezionabili in funzione dei requisiti tecnici e di business della Committente:

(a) Pull via API REST, con scheduling periodico (cron) o in modalità Near-Real-Time;

(b) Push via webhooks ed eventi, con notifiche server-to-server;

(c) Scambio file (CSV/JSON) su canali SFTP o S3-compatibili, con schema concordato tra le Parti;

(d) Integrazione tramite piattaforme iPaaS/ESB (a titolo esemplificativo: MuleSoft, Boomi) mediante connettori generici HTTP/REST;

(e) Single Sign-On per utenti interattivi (protocolli SAML 2.0 / OIDC), con provisioning automatizzato opzionale tramite protocollo SCIM.

8. Onboarding tecnico e deliverable

8.1 Il processo di onboarding tecnico comprende, salva diversa pattuizione nell'Ordine o nella SOW, le seguenti fasi e i relativi deliverable:

(a) Kick-off dell'integrazione e raccolta strutturata dei requisiti tecnici e di business;

(b) Redazione del Piano di Integrazione (perimetro dei flussi, mappatura dei campi, KPI, volumi stimati, finestre operative, responsabilità);

(c) Specifica tecnica (documentazione OpenAPI con esempi di payload, schemi dei file di scambio, contratti webhook);

(d) Configurazione (emissione credenziali, IP allowlist, parametri di sicurezza);

(e) Collaudo tecnico: test di connettività, autenticazione, flussi end-to-end, resilienza (retry e idempotenza);

(f) Go-live e avvio della fase di Hypercare, ove prevista dall'Ordine.

8.2 Con riferimento alla WMP, non è prevista una fase di UAT di processo: la piattaforma è configurata e resa disponibile alla Committente, che procede autonomamente al caricamento dei propri profili e dati. Eventuali fasi di UAT si applicano esclusivamente ove espressamente previste nell'Ordine o nella SOW con riferimento ad altri moduli (a titolo esemplificativo: VMP). Per TimeFlow Source non è prevista una fase di UAT di processo, salva diversa ed espressa pattuizione nell'Ordine.

9. Oneri economici

9.1 Gli oneri di seguito indicati hanno natura di catalogo e si applicano salva diversa pattuizione nell'Ordine, nella SOW o nel Listino Enterprise tempo per tempo vigente:

(a) Setup integrazione standard API/Webhook (una tantum): attivazione credenziali, configurazione profili di sicurezza e rate-limit, test con payload esemplificativi;

(b) Connettori e mapping: sviluppo o adeguamento di connettori, trasformazioni dati e mapping dei campi;

(c) Personalizzazioni applicative: estensioni di interfaccia utente o API, logiche di business specifiche, nuovi eventi;

(d) Exchange file gestito: definizione dello schema, validatori, controlli di qualità e schedulazioni;

(e) Supporto e Hypercare: assistenza tecnica post go-live entro la finestra temporale concordata;

(f) Manutenzione evolutiva: adeguamenti resi necessari da modifiche normative o tecniche di sistemi terzi.

9.2 La valorizzazione economica è definita nell'Ordine (a forfait ovvero a tempo e materiali). In assenza di specifica indicazione, la valorizzazione avviene a consuntivo secondo il Listino Enterprise vigente alla data di esecuzione (espresso in giornate/uomo ovvero in canoni mensili per connettori gestiti).

10. Assunzioni e prerequisiti della Committente

L'erogazione delle attività di integrazione presuppone, salva diversa pattuizione, il soddisfacimento dei seguenti prerequisiti a carico della Committente:

(a) disponibilità di un Identity Provider (IdP) per il Single Sign-On, ove richiesto; raggiungibilità degli endpoint di integrazione; messa a disposizione della documentazione tecnica dei sistemi terzi coinvolti;

(b) predisposizione di dati di prova non contenenti dati personali reali ovvero adeguatamente mascherati; nomina di utenti tecnici e di referenti IT e di processo dedicati;

(c) disponibilità di una finestra di test adeguata e, ove necessario, di ambienti sandbox dei sistemi terzi.

11. Limiti ed esclusioni

Salvo diverso accordo scritto tra le Parti, restano esclusi dal perimetro del presente Allegato: lo sviluppo di processi ETL complessi al di fuori del perimetro concordato; le migrazioni di dati storici; i test di sicurezza commissionati dalla Committente (cfr. MSA §2.5 e Allegato D §3); le licenze di software di terze parti; i connettori classificati come "premium" da fornitori terzi; la predisposizione di ambienti supplementari; il monitoraggio enterprise esteso (a titolo esemplificativo: integrazione con SIEM della Committente); le attività da svolgersi presso le sedi della Committente (onsite).

12. Variazioni (Change Request)

12.1 Qualsiasi modifica al perimetro, alle tempistiche, ai deliverable o ai prerequisiti di integrazione concordati è gestita mediante formale Change Request ("CR"). La CR descrive: (a) oggetto e motivazione della variazione; (b) impatti tecnici ed economici; (c) piano e tempistiche di esecuzione; (d) rischi e dipendenze.

12.2 L'esecuzione delle attività oggetto di CR è subordinata alla preventiva approvazione scritta della Committente. Fino a tale approvazione, restano validi il perimetro e le tempistiche originariamente concordati.

12.3 Le attività oggetto di CR sono valorizzate a forfait ovvero a tempo e materiali, secondo l'offerta o quotazione formulata da TimeFlow. Le variazioni possono comportare adeguamenti dei corrispettivi e delle milestone progettuali.

12.4 Per esigenze di urgenza debitamente motivate, le CR possono essere avviate sulla base di un'autorizzazione trasmessa via e-mail dalla Committente, con obbligo di formalizzazione della CR entro i successivi cinque (5) giorni lavorativi.

12.5 Restano esclusi dai livelli di servizio standard (SLA) gli elementi non ancora approvati o in corso di variazione, salvo diverso accordo scritto tra le Parti.

13. Accettazione e messa in esercizio

13.1 Integrazioni standard. L'accettazione tecnica delle integrazioni standard si perfeziona al superamento dei test concordati nel Piano di Integrazione. La messa in esercizio avviene a esito positivo dell'accettazione.

13.2 UAT di processo. La fase di User Acceptance Test non è prevista per la WMP e per TimeFlow Source, salva diversa ed espressa pattuizione. Per la VMP e per le personalizzazioni, la UAT si applica esclusivamente ove indicata nell'Ordine o nella SOW (cfr. MSA §4.5).

14. Supporto e SLA

14.1 Le API e i connettori sviluppati e mantenuti da TimeFlow rientrano nel perimetro dello SLA – Allegato C, con applicazione delle disposizioni in materia di finestre di manutenzione (§5), esclusioni (§6) e gestione degli incidenti (§7).

14.2 Per i componenti ospitati su infrastrutture della Committente, si applicano i livelli di servizio definiti dalla Committente medesima. I rimedi previsti dallo SLA (Service Credits) operano esclusivamente con riferimento ai componenti erogati e ospitati da TimeFlow (cfr. MSA §3.1 e Allegato C §§ 3–4).

15. Documentazione e tracciabilità

TimeFlow fornisce alla Committente la documentazione tecnica delle API in formato OpenAPI, esempi di request/response, guide di integrazione e changelog aggiornato. Tutte le chiamate API sono soggette ad audit trail e logging applicativo. È disponibile la telemetria per finalità di troubleshooting e per il monitoraggio dei KPI di integrazione (cfr. Allegato D §2.5).

16. 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. Nessun aggiornamento produce effetti retroattivi su attività già erogate o in corso di esecuzione.