ALLEGATO D — MISURE TECNICHE E ORGANIZZATIVE (TOMS) E BC/DR

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

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

Da sapere a colpo d'occhio

- Cifratura in transito e a riposo, chiavi gestite in KMS UE, MFA per gli accessi amministrativi, segregazione degli ambienti e logging centralizzato.
- Controlli periodici di sicurezza, comprensivi di vulnerability assessment automatizzato e verifiche manuali, con cadenza almeno annuale.
- Backup giornalieri cifrati in UE/SEE, test di restore trimestrali e obiettivi DR con RPO ≤ 30 minuti e RTO ≤ 8 ore (profilo standard).

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) e dello SLA (Allegato C).

- **Backup:** indica la copia di sicurezza periodica dei dati (completa o incrementale), conservata in forma cifrata, finalizzata a consentire il ripristino del Servizio e dei dati in caso di evento critico.
- **BC/DR (Business Continuity & Disaster Recovery):** indica l'insieme delle misure organizzative e tecniche volte a garantire la continuità operativa dei Servizi e il ripristino degli stessi a seguito di eventi critici o catastrofici.
- **Failover:** indica il passaggio controllato e automatico del carico di lavoro verso una risorsa o istanza alternativa in caso di guasto o degrado della componente primaria.
- **Fault Domain:** indica un insieme di risorse infrastrutturali che condividono un medesimo possibile punto di guasto; l'isolamento tra fault domain è finalizzato a ridurre l'impatto dei malfunzionamenti.
- **Hardening:** indica l'applicazione sistematica di configurazioni e controlli di sicurezza volti a ridurre la superficie d'attacco di sistemi, applicazioni e componenti infrastrutturali.
- **KMS (Key Management Service):** indica il servizio dedicato alla generazione, custodia, rotazione periodica e controllo degli accessi alle chiavi crittografiche utilizzate per la cifratura dei dati.

- **Least Privilege (Principio del Minimo Privilegio):** indica il criterio di assegnazione agli utenti e ai sistemi dei soli permessi strettamente necessari allo svolgimento delle rispettive attività, in conformità alle best practice di settore.
- **Multi-Tenant (Isolamento Multi-Tenant):** indica l'architettura in cui più tenant condividono la medesima infrastruttura applicativa, con isolamento logico dei dati e delle configurazioni a garanzia della segregazione.
- **NTP (Network Time Protocol):** indica il protocollo di sincronizzazione oraria utilizzato per allineare i clock dei sistemi, al fine di garantire la coerenza temporale dei log e delle registrazioni.
- **RPO (Recovery Point Objective):** indica l'intervallo massimo di dati che può essere perso in caso di evento catastrofico, espresso in unità temporali (obiettivo di punto di ripristino).
- **RTO (Recovery Time Objective):** indica il tempo massimo entro il quale il Servizio deve essere ripristinato a seguito di un evento catastrofico (obiettivo di tempo di ripristino).
- **Secure SDLC:** indica il ciclo di vita di sviluppo software che integra sistematicamente controlli di sicurezza in ciascuna fase (a titolo esemplificativo: code review, analisi statica e dinamica del codice, gestione delle dipendenze).
- **Segregazione degli Ambienti:** indica la separazione logica e fisica tra gli ambienti di sviluppo, test/UAT e produzione, con controlli di accesso e procedure di deployment distinti per ciascun ambiente.
- **Snapshot:** indica la cattura puntuale dello stato dei dati o dei volumi di storage, finalizzata ad accelerare le operazioni di backup e restore.
- **TOMs (Technical and Organisational Measures):** indica le misure tecniche e organizzative adottate da TimeFlow per la sicurezza delle informazioni e la conformità alla normativa applicabile.
- **Tombstoning:** indica il processo di marcatura e di eliminazione controllata e progressiva dei backup scaduti o non più necessari, nel rispetto delle policy di retention applicabili.
- **WAF (Web Application Firewall):** indica il sistema di controllo perimetrale che filtra, monitora e analizza il traffico HTTP/HTTPS diretto verso le applicazioni, al fine di rilevare e bloccare pattern di attacco e traffico malevolo.

1. Scopo, ambito e riferimenti

1.1 Finalità. Il presente Allegato definisce le Misure Tecniche e Organizzative (TOMs) adottate da TimeFlow per le Piattaforme TimeFlow, come definite nel MSA e individuate dai relativi Addenda di Prodotto (alla data della presente versione, WMP, VMP e TimeFlow Source), nonché i piani di Business Continuity e Disaster Recovery (BC/DR) applicabili all'erogazione dei Servizi.

1.2 Coordinamento contrattuale. Il presente Allegato si coordina con il MSA (in particolare §§ 3, 4, 7, 8, 9, 14, 15 e 18) e con lo SLA – Allegato C, con specifico riferimento a: oggetto e perimetro (§1), misurazione della disponibilità (§2), target e Service Credits

(§3), procedura di claim (§4), manutenzioni (§5), esclusioni (§6) e gestione degli incidenti (§7).

1.3 Ambito soggettivo. Le TOMs descritte nel presente Allegato si applicano esclusivamente a TimeFlow e alla sua organizzazione. Gli obblighi a carico della Committente restano quelli definiti nel MSA §7.

1.4 Ambito oggettivo. Il presente Allegato copre gli ambienti di produzione delle Piattaforme di cui al §1.1 e i connettori ufficiali sviluppati e mantenuti da TimeFlow. Gli ambienti sandbox e UAT hanno natura non produttiva ai sensi del MSA §2.8 e non sono destinati al trattamento di dati reali, salvo diverso accordo scritto tra le Parti con adozione di misure di sicurezza dedicate.

2. Misure tecniche e organizzative (TOMs)

2.1 Sicurezza dei dati

(a) Cifratura in transito e a riposo. Tutte le comunicazioni sono protette mediante protocollo TLS 1.2 o superiore, con abilitazione di HSTS ove applicabile. Tutti i dati persistenti, ivi inclusi quelli archiviati nei database e nei backup, sono cifrati mediante algoritmo AES-256 o equivalente.

(b) Gestione delle chiavi crittografiche. Le chiavi sono gestite tramite KMS con localizzazione in territorio UE/SEE, soggetto a rotazione con cadenza almeno annuale e on-demand in caso di compromissione; gli accessi al KMS sono segregati secondo il principio del minimo privilegio.

2.2 Controllo degli accessi e gestione delle identità

(a) Applicazione del principio del Least Privilege e della segregazione dei compiti; revisione periodica degli accessi con cadenza almeno semestrale.

(b) Autenticazione multifattore (MFA) obbligatoria per tutti gli account amministrativi di TimeFlow e per i canali di accesso privilegiato. Per gli Utenti Autorizzati della Committente, SSO e MFA sono disponibili ove abilitati (cfr. MSA §4.4).

(c) Politiche di gestione delle password e delle sessioni conformi alle best practice di settore (a titolo esemplificativo: complessità minima, scadenza, blocco per tentativi falliti, timeout di sessione).

2.3 Isolamento architetturale e infrastruttura

(a) Architettura multi-tenant con isolamento logico dei dati e delle configurazioni tra tenant distinti. Separazione rigorosa degli ambienti di sviluppo, test/UAT e produzione. La sicurezza fisica dell'infrastruttura è demandata al cloud provider, nel rispetto delle certificazioni indicate nell'Allegato G.

(b) Segmentazione di rete, WAF e controlli d'ingresso perimetrali; hardening dei sistemi conforme alle linee guida CIS Benchmarks ove applicabili.

(c) Storage e risorse computazionali localizzati in territorio UE/SEE. Eventuali trasferimenti extra-SEE sono ammessi esclusivamente ai sensi del MSA §8.3 e dell'Allegato G.

2.4 Sicurezza applicativa e SDLC

(a) Adozione di un ciclo di sviluppo sicuro (Secure SDLC) che integra: code review sistematiche, analisi statica e dinamica del codice (SAST/DAST), gestione delle dipendenze e verifica delle vulnerabilità note.

(b) Gestione dei segreti (credenziali, chiavi, token) tramite vault dedicato; nessun segreto è conservato in chiaro nel codice sorgente o nei file di configurazione.

(c) Sicurezza delle API: autenticazione tramite OAuth2/OpenID Connect o SAML 2.0; validazione dello schema delle richieste; rate-limit e throttling coerenti con il MSA §2.4; versionamento e gestione delle deprecazioni conformi al processo di change management di cui al MSA §9.5.

2.5 Logging, monitoraggio e osservabilità

(a) Log centralizzati (applicativi, di sicurezza e di audit) con sincronizzazione oraria tramite NTP.

(b) Sistemi di telemetria e alerting su eventi critici, con integrazione diretta nel processo di incident management disciplinato dallo SLA – Allegato C §7.

(c) Retention dei log: almeno centottanta (180) giorni per i log di sicurezza e audit, estendibile fino a dodici (12) mesi su richiesta motivata della Committente. I log sono conservati in forma cifrata e accessibili esclusivamente a ruoli autorizzati.

2.6 Dati non produttivi e minimizzazione

(a) Negli ambienti sandbox e UAT non è consentito il trattamento di dati reali della Committente, salvo diverso accordo scritto tra le Parti con adozione di misure di sicurezza dedicate (cfr. MSA §2.8).

(b) TimeFlow adotta il principio di minimizzazione dei dati, applicando tecniche di masking e pseudonimizzazione ove necessario.

2.7 Servizi di terze parti

L'erogazione di servizi accessori (a titolo esemplificativo: e-mail transazionali, gateway SMS) avviene tramite provider qualificati, i cui parametri contrattuali e livelli di disponibilità sono disciplinati dall'Allegato G e dalle esclusioni dello SLA (Allegato C §6).

3. Gestione delle vulnerabilità, patching e test di sicurezza

3.1 Gestione delle vulnerabilità. TimeFlow effettua scansioni continue delle vulnerabilità sui sistemi e sulle applicazioni. I tempi obiettivo per la remediation sono i seguenti: vulnerabilità critiche: entro sette (7) giorni; vulnerabilità alte: entro trenta (30) giorni; vulnerabilità medie: entro novanta (90) giorni; vulnerabilità basse: entro centottanta

(180) giorni. Sono ammesse mitigazioni compensative documentate in alternativa alla remediation diretta, ove questa non risulti immediatamente praticabile.

3.2 Patching. Gli aggiornamenti di sicurezza relativi a sistema operativo, middleware, database e componenti applicativi sono gestiti secondo una policy risk-based. Le finestre di manutenzione per il patching sono disciplinate dallo SLA – Allegato C §5.

3.3 Controlli periodici di sicurezza. TimeFlow effettua controlli periodici di sicurezza, comprensivi di vulnerability assessment automatizzato e verifiche manuali, con cadenza almeno annuale. L'executive summary dell'ultimo ciclo di controlli è condivisibile con la Committente su richiesta, previa oscurazione dei dettagli sensibili relativi all'infrastruttura (cfr. MSA §9.4).

3.4 Sicurezza della supply chain. TimeFlow conduce attività di due diligence sui fornitori critici e sulle componenti open-source (OSS). La distinta delle dipendenze software (SBOM) è mantenuta aggiornata. Sono adottati controlli di integrità su immagini e container.

3.5 Resilienza e rate-limiting. TimeFlow implementa meccanismi di enforcement dei rate-limit, degradazione controllata del servizio (tramite cache, code, back-pressure) e blocchi proporzionati del traffico malevolo o riconducibile ad attacchi DoS/DDoS. Le fattispecie escluse dal computo della disponibilità sono quelle indicate nello SLA – Allegato C §6.

4. Incident response, comunicazioni e data breach

4.1 Processo di gestione degli incidenti. Gli incidenti sono gestiti attraverso un processo strutturato di rilevazione, triage e classificazione della severità (SEV-1/2/3/4), con tempi di Ack, aggiornamento, workaround e ripristino definiti nello SLA – Allegato C §7.

4.2 Notifiche e tempistiche. (a) Gli avvisi operativi relativi agli incidenti sono trasmessi tramite i canali previsti nello SLA – Allegato C §9. Il Reason For Outage (RFO) è comunicato entro ventiquattro (24) ore dal ripristino; la Root Cause Analysis (RCA) è comunicata entro cinque (5) o dieci (10) giorni lavorativi, secondo la severità dell'incidente, come disciplinato dallo SLA – Allegato C §7. (b) Per gli incidenti che coinvolgano Dati Personali della Committente, la notifica è effettuata senza ingiustificato ritardo e, comunque, entro settantadue (72) ore dalla conoscenza dell'evento (cfr. MSA §8.5 e DPA – Allegato B, art. 3.1(e)).

4.3 Evidenze e forensics. TimeFlow provvede alla conservazione dei log e al mantenimento della catena di custodia delle evidenze digitali. TimeFlow presta ragionevole cooperazione nei confronti delle Autorità competenti e degli Interessati, per quanto di propria competenza (cfr. MSA §8.6).

4.4 Clock-Stop e dipendenze da terzi. I timer operativi di cui allo SLA – Allegato C §7 si sospendono in caso di attesa di informazioni, asset o risposte da parte della Committente, ovvero per dipendenze da fornitori terzi, come definito nello SLA (Definizioni: "Clock-Stop" e §6, lett. l).

5. Business Continuity & Disaster Recovery

5.1 Architettura e continuità. L'architettura infrastrutturale è progettata per garantire ridondanza delle componenti critiche, backup e snapshot cifrati, isolamento tra fault domain e piani di failover documentati e testati.

5.2 Backup e restore. (a) Backup: eseguiti con cadenza almeno giornaliera (full e/o incrementali), con periodo di retention minimo di trenta (30) giorni, conservati in forma cifrata in territorio UE/SEE. (b) Test di restore: eseguiti con cadenza almeno trimestrale su dataset rappresentativi; le evidenze dei test sono disponibili su richiesta della Committente.

5.3 Obiettivi di ripristino (DR). I seguenti obiettivi si applicano in caso di evento catastrofico:

Profilo	RPO	RTO
Standard	≤ 30 minuti	≤ 8 ore
Alta disponibilità (se in Ordine)	≤ 15 minuti	≤ 4 ore

Gli obiettivi di DR sono distinti e separati dai target operativi di gestione degli incidenti disciplinati dallo SLA – Allegato C §7.

5.4 Esercitazioni DR. TimeFlow effettua esercitazioni di disaster recovery con cadenza almeno annuale, mediante simulazioni table-top e/o test tecnici. Eventuali scostamenti rilevati sono oggetto di piano CAPA e di azioni correttive documentate.

5.5 Dipendenze da provider terzi. Le interruzioni del servizio esclusivamente imputabili al cloud provider o a fornitori di servizi esterni rientrano nelle Esclusioni dello SLA (Allegato C §6). Resta fermo l'obbligo di TimeFlow di attivare le misure di mitigazione e i piani BC/DR previsti dal presente Allegato.

5.6 Rollback e coerenza dei dati. In caso di change non riuscito o di difetto bloccante, TimeFlow esegue il rollback alla versione precedente ove tecnicamente possibile, con priorità alla salvaguardia dell'integrità e della tracciabilità dei dati (cfr. MSA §9.5).

6. Ciclo di vita dei dati, portabilità e strategie di exit

6.1 Portabilità e export. Alla cessazione del MSA o del singolo Ordine, su richiesta della Committente formulata entro trenta (30) giorni dalla data di efficacia della cessazione, TimeFlow rende disponibile un export una tantum dei Dati della Committente in formato CSV e/o JSON, corredato da dizionario dei campi, fatte salve le disposizioni del DPA – Allegato B, art. 6, e, per le Committenti soggette al DORA, dell'Allegato E, §5.7 (cfr. MSA §8.7). Formati di export ulteriori, estrazioni personalizzate e servizi di assistenza all'exit sono disponibili a quotazione separata.

6.2 Cancellazione e tombstoning dei backup. Decorso il termine di cui al precedente comma 6.1, ovvero in caso di mancata richiesta di export, TimeFlow provvede alla

cancellazione dei Dati della Committente e al tombstoning progressivo dei backup secondo le policy di retention applicabili. Su richiesta, TimeFlow rilascia alla Committente apposita attestazione di avvenuta cancellazione (cfr. MSA §8.7).

6.3 Retention operativa. I dati applicativi della Committente sono conservati per l'intera durata del Servizio. Per le retention specifiche dei log tecnici e di sicurezza si rinvia al §2.5 del presente Allegato. Per TimeFlow Source, i Dati di Contatto Nominativi sono cancellati automaticamente decorsi dodici (12) mesi dall'ultima operazione che li ha interessati, secondo quanto previsto dall'Appendice 2 al DPA, Art. 6.1.

6.4 Dati di categorie particolari. È fatto divieto alla Committente di immettere nelle Piattaforme dati appartenenti a categorie particolari ai sensi dell'art. 9 del GDPR o dati relativi a condanne penali e reati ai sensi dell'art. 10 del GDPR, salvo quanto diversamente ed espressamente previsto nel MSA §8.9 e nel DPA (per le Piattaforme per le quali TimeFlow opera quale responsabile del trattamento, VMP e TimeFlow Source) o nell'informativa privacy (per la WMP).

6.5 Export e copie locali della Committente. Gli export e le copie locali dei dati estratti dalle Piattaforme dalla Committente restano sotto l'esclusiva responsabilità di quest'ultima per quanto attiene alla sicurezza, alla conservazione e alla retention (cfr. MSA §7).

7. Fornitori esterni, trasferimenti e audit

7.1 Subfornitori e localizzazione. L'elenco dei subfornitori e le relative regole di variazione sono disciplinati nell'Allegato G. Le notifiche di variazione e il diritto di opposizione (per le Piattaforme per le quali TimeFlow opera quale responsabile del trattamento, VMP e TimeFlow Source) sono regolati dal MSA §15. TimeFlow garantisce il flow-down degli obblighi di sicurezza e protezione dei dati personali a tutti i subfornitori, conformemente al MSA §15.

7.2 Trasferimenti extra-SEE. Eventuali trasferimenti di dati verso Paesi al di fuori dello Spazio Economico Europeo sono ammessi esclusivamente ai sensi del Capo V del GDPR, con adozione delle Clausole Contrattuali Standard (SCC) e delle misure supplementari applicabili, come disciplinato dal MSA §8.3 e dall'Allegato G.

7.3 Audit e trasparenza. La Committente può richiedere la compilazione di questionari di sicurezza, la produzione di attestazioni e l'esecuzione di audit documentali o on-site, nei termini e con le modalità stabiliti dal MSA §9.4, nel rispetto degli obblighi di riservatezza di cui al MSA §13.

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. Nessun aggiornamento ha efficacia retroattiva.