ALLEGATO E — COMPLIANCE NIS2 · DORA · AI ACT — WORKFORCE MANAGEMENT PLATFORM (WMP)

Ultima modifica: 08/07/2026 | Versione: COMP-WMP-2026-07-08

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

Da sapere a colpo d'occhio

- Impegni di cooperazione NIS2 e DORA, con notifica incidenti in 24/72 ore, pacchetto annuale di evidenze e supporto al Register of Information.
- Inventario AI Act della WMP: CV Parser ed Estrazione Competenze, Matching Recruiting ibrido (layer semantico disattivato di default), Caricamento via Email e Arricchimento Competenze a rischio limitato (art. 50); componenti di Scheduling deterministici, non sistemi di IA. TimeFlow opera quale titolare autonomo (Addendum WMP, Art. 2).
- Trasparenza ex art. 50 dal 2 agosto 2026; monitoraggio della classificazione in ambito occupazionale verso il regime Allegato III del 2 dicembre 2027 (Digital Omnibus); nessun modello addestrato con dati della Committente.

1. Scopo e ambito di applicazione

1.1 Finalità. Il presente Allegato disciplina gli impegni di cooperazione e le misure adottate da TimeFlow al fine di supportare la Committente nell'adempimento degli obblighi derivanti dalla normativa europea in materia di sicurezza delle reti e dei sistemi informativi (Direttiva (UE) 2022/2555 – «NIS2»), di resilienza operativa digitale del settore finanziario (Regolamento (UE) 2022/2554 – «DORA») e di intelligenza artificiale (Regolamento (UE) 2024/1689 – «AI Act»), nella misura in cui tali normative siano applicabili alla Committente e/o ai Servizi erogati da TimeFlow.

1.2 Natura dell'Allegato. Le disposizioni del presente Allegato integrano, senza sostituire, gli obblighi già previsti dal MSA, dagli Addenda di Prodotto e dagli altri Allegati. Ove non diversamente ed espressamente previsto, i termini con lettera iniziale maiuscola hanno il significato attribuito nel MSA (Allegato A).

1.3 Attivazione. Il presente Allegato si applica nella misura in cui la Committente sia soggetta, direttamente o in qualità di fornitore ICT di entità regolamentate, agli obblighi derivanti dalla NIS2, dal DORA e/o dall'AI Act. L'applicabilità è indicata nell'Ordine ovvero comunicata per iscritto dalla Committente.

1.4 Coordinamento contrattuale. Il presente Allegato si coordina in particolare con: MSA §§ 3, 7, 8, 9, 14, 15 e 18; Addendum di Prodotto – WMP; SLA – Allegato C; TOMs & BC/DR – Allegato D; Elenco fornitori – Allegato G.

1.5 Ambito di Piattaforma. Il presente Allegato si riferisce alla Workforce Management Platform («WMP»). Ove l'Ordine attivi più Piattaforme, a ciascuna si applica il rispettivo Allegato E di Piattaforma, nelle Versioni Pinnate indicate nell'Ordine.

SEZIONE I — DIRETTIVA NIS2 (UE) 2022/2555

2. Sicurezza della supply chain (art. 21, par. 2, lett. d, NIS2)

2.1 Impegno generale. TimeFlow si impegna a mantenere misure tecniche, operative e organizzative adeguate per la gestione dei rischi per la sicurezza delle reti e dei sistemi informativi utilizzati nell'erogazione dei Servizi, in coerenza con l'art. 21 della Direttiva NIS2 e con le relative disposizioni di recepimento nazionale.

2.2 Cooperazione per la valutazione del rischio di supply chain. Su richiesta motivata della Committente, TimeFlow collabora ragionevolmente nelle attività di risk assessment relative alla supply chain ICT, fornendo le informazioni necessarie alla Committente per la valutazione del rischio associato ai Servizi erogati, ivi incluse: (a) la descrizione dell'architettura di sicurezza; (b) le certificazioni e attestazioni vigenti (cfr. MSA §9.1–9.4); (c) l'elenco dei sub-fornitori critici e le relative misure di sicurezza (cfr. Allegato G).

2.3 Standard e certificazioni. TimeFlow mantiene le certificazioni ISO/IEC 27001 e ISO 9001 (cfr. MSA §9.1). Su richiesta ragionevole, TimeFlow rende disponibili alla Committente: (a) il certificato ISO 27001 aggiornato e la relativa Dichiarazione di Applicabilità (SoA); (b) l'executive summary dell'ultimo penetration test (cfr. Allegato D §3.3); (c) l'evidenza dei test di restore (cfr. Allegato D §5.2); (d) lo stato del patching e della remediation delle vulnerabilità (cfr. Allegato D §3.1–3.2). Tali documenti costituiscono Informazioni Riservate del Fornitore ai sensi del MSA §13.

3. Notifica degli incidenti (art. 23 NIS2)

3.1 Early warning. In caso di incidente significativo che possa avere impatto sulla sicurezza delle reti e dei sistemi informativi della Committente ovvero sulla continuità dei Servizi, TimeFlow trasmette alla Committente un'allerta preliminare (early warning) entro ventiquattro (24) ore dalla rilevazione dell'evento, contenente almeno: (a) la natura dell'incidente e la sua classificazione di severità; (b) una prima valutazione dell'impatto potenziale; (c) le misure di contenimento già adottate.

3.2 Notifica completa. Entro settantadue (72) ore dalla rilevazione, TimeFlow trasmette alla Committente una notifica dettagliata comprensiva di: (a) descrizione della natura e delle cause dell'incidente; (b) valutazione dell'impatto effettivo sui Servizi e, ove noto, sui dati della Committente; (c) misure adottate e piano delle azioni correttive (CAPA); (d) riferimenti ai ticket e alla timeline dell'evento.

3.3 Report finale. Per gli incidenti di severità SEV-1 e SEV-2, TimeFlow fornisce un report finale (Root Cause Analysis) nei termini previsti dallo SLA – Allegato C §7.3.

3.4 Coordinamento con la notifica GDPR. La notifica di cui al presente articolo non sostituisce né pregiudica gli obblighi di notifica in materia di violazione dei dati personali (Data Breach) previsti dal MSA §8.5 e, ove applicabile ai trattamenti eseguiti per conto della Committente, dal DPA – Allegato B, art. 3.1(e). Ove l'incidente coinvolga Dati Personali, si applicano congiuntamente entrambe le procedure.

3.5 Ambito. Ai fini del presente articolo, per «incidente significativo» si intende qualsiasi evento che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei Servizi o dei dati trattati, con impatto potenziale sulla Committente, e che non rientri tra le ordinarie anomalie coperte dai processi di incident management dello SLA.

4. Audit, evidenze e cooperazione con le Autorità NIS2

4.1 Audit regolamentare. In aggiunta ai diritti di audit previsti dal MSA §9.4, qualora la Committente sia soggetta ad attività di verifica, ispezione o indagine da parte dell'Autorità competente NIS2 (in Italia: Agenzia per la Cybersicurezza Nazionale – ACN), TimeFlow presta ragionevole cooperazione, nei limiti di quanto attinente ai Servizi erogati, ivi inclusa la messa a disposizione di documentazione, log e risposte a questionari dell'Autorità. I relativi audit regolamentari non sono computati nel limite annuale di cui al MSA §9.4.

4.2 Pacchetto periodico di evidenze. TimeFlow si impegna a rendere disponibile alla Committente, con cadenza almeno annuale e su richiesta motivata, un pacchetto sintetico di evidenze di conformità comprensivo di: (a) certificato ISO 27001 vigente; (b) executive summary del pen-test annuale; (c) stato delle vulnerabilità critiche e alte; (d) esito dei test di restore DR; (e) elenco aggiornato dei sub-fornitori (Allegato G). Tali documenti sono classificati come Informazioni Riservate.

4.3 Formazione e awareness del personale. TimeFlow garantisce che il proprio personale coinvolto nell'erogazione dei Servizi riceva formazione periodica in materia di sicurezza informatica, in coerenza con i requisiti del proprio SGSI (cfr. MSA §9.1).

4.4 Flow-down NIS2 ai subfornitori. TimeFlow impone ai propri subfornitori critici obblighi di sicurezza coerenti con le misure di gestione del rischio previste dalla NIS2, e ne verifica periodicamente la conformità (cfr. Allegato G §4).

SEZIONE II — REGOLAMENTO DORA (UE) 2022/2554

5. Clausole contrattuali DORA (art. 30)

5.1 Ambito. Le disposizioni della presente Sezione II si applicano nella misura in cui la Committente sia un'entità finanziaria soggetta al DORA, ovvero un fornitore ICT di entità finanziarie soggette al DORA, e i Servizi erogati da TimeFlow supportino funzioni critiche o importanti della Committente. L'applicabilità è indicata nell'Ordine.

5.2 Descrizione completa dei Servizi (art. 30.2(a)(b)). La descrizione dei Servizi ICT forniti, la localizzazione dei dati e l'indicazione delle condizioni di subappalto sono contenute nel MSA (§§1–2), nell'Addendum di Prodotto, nell'Ordine e nell'Allegato G. Su richiesta, TimeFlow fornisce una mappatura supplementare dei Servizi ICT in relazione alle funzioni critiche o importanti della Committente, al fine di alimentare il Register of Information di cui all'art. 28, par. 3, del DORA.

5.3 Livelli di servizio (art. 30.3(a)). I livelli di servizio sono definiti nello SLA – Allegato C con target quantitativi e qualitativi misurabili. I Service Credits costituiscono il rimedio contrattuale esclusivo per gli scostamenti dai livelli pattuiti (cfr. MSA §3.1 e SLA §3). La Committente ha facoltà di monitorare l'adeguatezza dei Servizi tramite le metriche e i report previsti dal MSA §2.6 e dallo SLA §9.

5.4 Assistenza in caso di incidenti ICT (art. 30.2(f)). In caso di incidente ICT relativo ai Servizi, TimeFlow presta alla Committente assistenza nella gestione, nella diagnosi e nella risoluzione dell'incidente, senza costi aggiuntivi e nell'ambito dei canoni già previsti dall'Ordine, con i tempi e le modalità indicati nello SLA – Allegato C §7. Sono fatti salvi i corrispettivi per eventuali attività di assistenza straordinaria eccedenti il perimetro ordinario, ove preventivamente concordate per iscritto.

5.5 Business continuity e piani di contingenza (art. 30.3(b)(c)). I piani di business continuity e disaster recovery sono descritti nell'Allegato D §5, con obiettivi di RPO/RTO quantificati. TimeFlow effettua esercitazioni DR con cadenza almeno annuale (cfr. Allegato D §5.4). TimeFlow notifica tempestivamente alla Committente qualsiasi sviluppo che possa avere un impatto rilevante sulla propria capacità di erogare i Servizi in conformità ai livelli di servizio pattuiti.

5.6 Audit e accesso alle informazioni (art. 30.3(e)). La Committente ha diritto di effettuare audit, ispezioni e accesso alle informazioni relative ai Servizi secondo le modalità previste dal MSA §9.4. Ove i Servizi supportino funzioni critiche o importanti, TimeFlow collabora con le autorità di vigilanza finanziaria della Committente (a titolo esemplificativo: Banca d'Italia, CONSOB, IVASS) nella misura in cui queste richiedano informazioni o verifiche sui Servizi ICT erogati. I diritti di audit regolamentari non sono soggetti al limite annuale ordinario di cui al MSA §9.4.

5.7 Strategia di exit e portabilità (art. 30.3(f)(g)). 5.7.1 Alla cessazione del rapporto contrattuale, per qualsiasi causa, TimeFlow garantisce un periodo di transizione di almeno novanta (90) giorni (o il diverso periodo indicato nell'Ordine) durante il quale i Servizi continuano ad essere erogati alle medesime condizioni, al fine di consentire alla Committente la migrazione verso un fornitore alternativo o una soluzione interna. 5.7.2 Durante il periodo di transizione, TimeFlow: (a) rende disponibile l'export dei dati (personali e non personali) in formato CSV e/o JSON, corredato da dizionario dei campi (cfr. MSA §8.7); (b) presta ragionevole assistenza alla migrazione, su richiesta della Committente e a condizioni economiche concordate mediante SOW dedicata; (c) garantisce la restituzione e/o la cancellazione dei dati secondo le modalità previste dal MSA §8.7 e dall'Allegato D §6. 5.7.3 In caso di insolvenza, cessazione delle attività o

risoluzione del rapporto contrattuale per fatto del Fornitore, TimeFlow si impegna ad assicurare, nei limiti di quanto ragionevolmente possibile, l'accessibilità e la restituzione dei dati della Committente e la continuità dei Servizi per il periodo strettamente necessario alla migrazione.

5.8 Cooperazione con le autorità di vigilanza (art. 30.2(g)). TimeFlow si impegna a cooperare pienamente con le autorità competenti di vigilanza e di risoluzione della Committente, ivi incluse le persone da queste designate, nella misura prevista dalla normativa applicabile e limitatamente all'ambito dei Servizi erogati.

5.9 Partecipazione a programmi di resilienza (art. 30.2(h) e art. 13(6)). TimeFlow si impegna a partecipare ragionevolmente, su invito della Committente e con cadenza non superiore a due (2) occasioni per anno solare, a iniziative di awareness, formazione o simulazione in materia di resilienza operativa digitale organizzate dalla Committente, nei limiti di quanto pertinente ai Servizi erogati.

5.10 Register of Information (art. 28, par. 3, DORA). Su richiesta della Committente, TimeFlow fornisce le informazioni necessarie alla compilazione e all'aggiornamento del Register of Information previsto dall'art. 28, par. 3, del DORA, ivi incluse: la descrizione dei Servizi ICT, la localizzazione dei dati e delle infrastrutture, l'indicazione dei sub-fornitori e la classificazione di criticità dei Servizi.

SEZIONE III — REGOLAMENTO AI ACT (UE) 2024/1689

6. Componenti algoritmici e di intelligenza artificiale della WMP

6.1 Criteri dell'inventario e quadro temporale. 6.1.1 Alla data del presente Allegato, la WMP integra i componenti algoritmici e di intelligenza artificiale descritti nella presente Sezione. L'inventario distingue: (a) i componenti inclusi nella dotazione della Piattaforma secondo l'Ordine; (b) i componenti disponibili esclusivamente previa attivazione del relativo modulo opzionale mediante Ordine o SOW integrativo. 6.1.2 I componenti di intelligenza artificiale operano mediante modelli di fornitori terzi. L'individuazione puntuale dei fornitori di modelli, dei servizi utilizzati e delle relative garanzie (localizzazione dell'elaborazione, conservazione, esclusione dei dati della Committente dall'addestramento) è contenuta, quale fonte contrattualmente vincolante, nell'Allegato G, Tabella B. Nessun modello è addestrato da TimeFlow e nessun dato della Committente è utilizzato per l'addestramento dei modelli dei fornitori. 6.1.3 La Committente può limitare i motori di intelligenza artificiale utilizzabili nel proprio tenant ai sensi dell'Allegato G, §3.5. 6.1.4 Quadro temporale. Gli obblighi di trasparenza di cui all'art. 50 del Regolamento (UE) 2024/1689 si applicano dal 2 agosto 2026; il regime dei sistemi ad alto rischio di cui all'Allegato III del medesimo Regolamento si applica dal 2 dicembre 2027, per effetto del differimento disposto dal pacchetto di semplificazione europeo («Digital Omnibus») adottato il 7 maggio 2026. TimeFlow monitora la relativa evoluzione ai sensi del §10.1.

6.2 Inventario sinottico.

Componente	Classificazione AI Act	Disponibilità
AI Talent Match Insights (Matching 2.0)	Sistema di IA a rischio limitato (art. 50)	Modulo opzionale (solo se incluso nell'Ordine)
Data Mining – CV Parser ed Estrazione Competenze	Sistema di IA a rischio limitato (art. 50)	Incluso / secondo Ordine
Componenti deterministici di Scheduling	Non costituiscono sistemi di IA	Inclusi (WMP base)
Matching Avanzato – Recruiting	Nucleo deterministico; layer semantico opzionale (ove attivato: IA a rischio limitato)	Secondo Ordine; layer disattivato per impostazione predefinita
Caricamento posizioni e profili tramite Email (AI)	Sistema di IA a rischio limitato (art. 50)	Secondo Ordine
Arricchimento automatico Nuove Competenze (AI)	Sistema di IA a rischio limitato (art. 50)	Secondo Ordine
Agentic AI Collaborator (AI Agent Builder)	Sistema di IA a rischio limitato (art. 50)	Modulo opzionale (Ordine/SOW dedicato)

6.3 Componenti della Piattaforma

6.3.0 Ruolo privacy. Con riferimento ai trattamenti di dati personali connessi ai componenti della presente Sezione, TimeFlow opera quale titolare autonomo del trattamento ai sensi dell'Addendum di Prodotto — WMP, Art. 2, e rende le relative informative direttamente agli interessati ai sensi degli artt. 13 e 14 GDPR.

AI Talent Match Insights — Matching 2.0 (modulo opzionale). Le disposizioni del presente paragrafo si applicano esclusivamente ove la Committente abbia attivato il modulo «AI Talent Match Insights» mediante indicazione nell'Ordine. (a) Natura del componente. L'AI Talent Match Insights è un sistema di intelligenza artificiale ai sensi dell'art. 3, n. 1, del Regolamento AI Act. Il sistema effettua un'analisi dettagliata della compatibilità tra i requisiti progettuali della Committente e i profili professionali disponibili, fornendo insight analitici avanzati rispetto al matching di base, mediante elaborazione semantica basata su modelli LLM di terze parti; al fornitore del modello è trasmesso il testo estratto dai documenti e dai profili oggetto di analisi. (b) Classificazione del rischio. Il sistema è classificato a rischio limitato ai sensi dell'art. 50 del Regolamento AI Act. L'output è di natura analitica e di supporto decisionale: nessuna decisione è assunta autonomamente. L'operatore umano è sempre il decisore finale (human-in-the-loop). (c) Trasparenza. TimeFlow garantisce la trasparenza circa l'utilizzo di componenti AI, mettendo a disposizione della Committente la documentazione tecnica e le istruzioni d'uso.

6.3.2 Modulo Data Mining — CV Parser ed Estrazione Competenze. (a) Natura del componente. Il componente estrae in forma strutturata i dati curriculari dai CV caricati sulla Piattaforma (PDF, DOC o immagine tramite OCR) e ne popola i campi del profilo, riducendo tempi di data entry ed errori manuali. La pipeline combina parsing

deterministico (OCR e pattern matching lessicale) e, per l'analisi semantica delle competenze e per l'anonimizzazione dei CV, modelli LLM di terze parti, ai quali è trasmesso il testo del CV (nei limiti dei primi 12.000 caratteri) unitamente alla tassonomia delle competenze; l'output è il profilo strutturato (competenze e livello, esperienze, istruzione, certificazioni, lingue, seniority). I dati trasmessi possono includere dati personali contenuti nel CV. (b) Minimizzazione e controllo umano. Il parser popola esclusivamente i campi strettamente necessari al completamento del profilo; gli ulteriori dati presenti nei CV sono scartati; il testo trasmesso è troncato nei limiti sopra indicati; il form può essere compilato interamente a mano in alternativa all'estrazione automatica e l'utente può modificare o integrare i dati estratti prima del salvataggio (revisione umana). (c) Addestramento. La componente di parsing deterministico è stata sviluppata mediante apprendimento supervisionato su un dataset controllato, statico e non riconducibile a persone fisiche identificate o identificabili; il sistema non è addestrato tramite i dati di utilizzo, e restano ferme le garanzie del §6.1.2 quanto ai modelli di terze parti.

6.3.3 Componenti deterministici di Scheduling. L'Analisi Compatibilità Profili, l'Allocazione Intelligente e l'Ottimizzazione Costi Allocazioni operano mediante algoritmi deterministici eseguiti localmente (punteggi pesati su competenze, seniority, certificazioni, vincoli di sede e modalità; controlli transazionali di saturazione; calcoli aritmetici dei risparmi), riutilizzando dati già presenti nella Piattaforma. Nessun dato è trasmesso a fornitori esterni e nessun modello linguistico è invocato. Tali componenti non presentano capacità inferenziale (Considerando 12 AI Act), non sono oggetto di addestramento e producono output formalmente determinati: non costituiscono sistemi di IA ai sensi dell'art. 3, n. 1, del Regolamento. TimeFlow adotta su base volontaria documentazione tecnica su richiesta, indicazione della natura algoritmica dell'output e piena ricostruibilità dell'output dai dati di input e dalle regole di calcolo.

6.3.4 Matching Avanzato — Recruiting. Il componente si articola in un nucleo deterministico eseguito localmente (analisi testuale TF-IDF), che non comporta alcuna trasmissione di dati a fornitori esterni, e in un layer semantico opzionale, disattivato per impostazione predefinita. Ove il layer sia espressamente abilitato, sono trasmessi al fornitore del modello, per la sola generazione di rappresentazioni vettoriali (embeddings), il testo della posizione (titolo, descrizione, competenze, seniority, dominio) e il testo del CV del candidato (nei limiti dei primi 8.000 caratteri); il ricalcolo dei punteggi è eseguito localmente. Ove attivato, il layer costituisce sistema di IA a rischio limitato ai sensi dell'art. 50.

6.3.5 Caricamento posizioni e profili tramite Email (AI). Il componente struttura automaticamente posizioni e profili a partire dalle email ricevute: sono trasmessi al fornitore del modello l'oggetto e il corpo dell'email, il testo estratto localmente dagli allegati (PDF, DOCX, TXT) e, per i profili candidato, l'indirizzo email del mittente e il testo del CV, nei limiti dei primi 12.000 caratteri. I dati trasmessi possono includere dati personali. L'esito è sottoposto a revisione umana prima dell'inserimento definitivo.

6.3.6 Arricchimento automatico Nuove Competenze (AI). Il componente integra la tassonomia delle competenze: sono trasmessi al fornitore del modello esclusivamente il nome della competenza e la relativa categoria; nessun CV, nessun dato personale e nessun testo di posizione. Il modello restituisce sinonimi e competenze correlate, integrati nella tassonomia.

6.3.7 Garanzie comuni della Sezione. Per tutti i componenti della presente Sezione: (a) l'output ha natura di supporto informativo e la decisione finale è rimessa a un operatore umano; nessuna decisione automatizzata produce effetti giuridici sugli interessati; (b) restano ferme le misure dei §§7, 8 e 9 e le garanzie sui fornitori di modelli di cui al §6.1.2; (c) in considerazione dell'impiego in ambito di gestione del personale e selezione, TimeFlow monitora la classificazione dei componenti ai sensi dell'art. 6 e dell'Allegato III del Regolamento AI Act, anche in vista del regime applicabile dal 2 dicembre 2027 (§6.1.4), documenta le relative valutazioni e le rende disponibili alla Committente su richiesta.

6.4 Agentic AI Collaborator (modulo opzionale trasversale)

Le disposizioni del presente paragrafo 6.4 e dei successivi §§ 7, 8 e 9 si applicano, per le parti relative all'Agentic AI Collaborator, esclusivamente ove attivato mediante Ordine o SOW integrativo.

6.4.1 Natura del componente. L'Agentic AI Collaborator è un sistema di intelligenza artificiale ai sensi dell'art. 3, n. 1, del Regolamento AI Act, che opera come orchestratore agnostico rispetto ai modelli LLM sottostanti, consentendo alla Committente di interrogare in linguaggio naturale le proprie basi dati (Text-to-SQL) e documentazione (RAG).

6.4.2 Classificazione. Sistema di IA a rischio limitato (art. 50 AI Act), sulla base di Risk Assessment formale ex art. 9 su tre casi d'uso (Procurement, Legal, Audit), ciascuno con rischio residuo BASSO. Non GPAI. Esclusione Allegato III punto 5(a) documentata per Procurement (art. 6(3)).

6.4.3 Provider LLM (tutti con EU data residency). (a) OpenAI (OpenAI Ireland Ltd.; EU data residency via eu.api.openai.com; zero data retention; SOC 2 Type II, ISO 27001); (b) Anthropic (DPA con SCC; retention API 7gg; inference EU tramite AWS Bedrock regioni EU — eu-central-1 Francoforte, eu-west-1 Irlanda — con zero data retention in Bedrock); (c) Google (Vertex AI EU — europe-west3 Francoforte / europe-west4 Paesi Bassi; dati non usati per training; data residency garantita per endpoint regionali). Nessun modello addestrato da TimeFlow.

6.4.4 Supervisione umana. Human-in-the-loop by design: non compie azioni autonome, non modifica dati, output esclusivamente informativo. Feedback loop, richiesta chiarimenti, citazione fonti.

6.4.5 Auditabilità. Framework audit multi-livello: audit log, LLM call log (prompt/risposta/provider/token/latenza), agent runs, request ID univoco, conversation history, tracciamento fonti RAG.

6.4.6 Trasparenza (art. 50). Documentazione tecnica, Risk Assessment formale, istruzioni d'uso disponibili alla Committente.

7. Allocazione dei ruoli AI Act

7.1 Ruoli per componente. (a) Per i componenti che non costituiscono sistemi di IA: non applicabile; (b) per i componenti di intelligenza artificiale di cui al §6.3: TimeFlow fornitore, Committente deployer; (c) per l'Agentic AI Collaborator (ove attivato): TimeFlow fornitore ex art. 3(3), Committente deployer ex art. 3(4).

7.2 Obblighi del fornitore. TimeFlow si obbliga a: (a) mantenere documentazione tecnica aggiornata; (b) comunicare modifiche sostanziali con preavviso ragionevole; (c) cooperare per obblighi di trasparenza; (d) monitorare il funzionamento; (e) rendere disponibile la Risk Assessment aggiornata (Agentic AI Collaborator).

7.3 Obblighi del deployer. La Committente si obbliga a: (a) utilizzare i componenti AI conformemente alle istruzioni e all'AUP; (b) sottoporre l'output a supervisione umana prima di decisioni con effetti sugli Interessati; (c) non utilizzare l'output quale unico criterio decisionale per qualificazione, esclusione o de-listing fornitori, decisioni in materia di personale, decisioni legali vincolanti, o audit conclusivi; (d) non apportare modifiche che alterino sostanzialmente finalità, logica o rischio (art. 25 AI Act) senza accordo scritto.

7.4 Variazione della classificazione. Qualora l'utilizzo configuri un sistema ad alto rischio (art. 6 e Allegato III AI Act), la Committente comunica tempestivamente a TimeFlow. Le Parti cooperano per le misure necessarie, inclusa eventuale sottoscrizione di accordo integrativo.

8. AI literacy e formazione (art. 4 AI Act)

8.1 Componenti non costituenti sistemi di IA. TimeFlow mette a disposizione, su richiesta, la documentazione tecnica descrittiva.

8.2 Componenti di intelligenza artificiale. Per i componenti di IA di cui alla presente Sezione III (ove attivati): (a) documentazione tecnica; (b) formazione di primo avviamento (ove prevista); (c) linee guida sull'uso responsabile dell'output AI e sulla supervisione umana, ai sensi dell'art. 4 AI Act.

9. Monitoraggio e aggiornamenti dei componenti

9.1 Componenti deterministici. Soggetti a manutenzione ordinaria. Modifiche a logica di calcolo, criteri di estrazione o dataset di training comunicate nelle release notes.

9.2 Componenti di intelligenza artificiale. Monitoraggio continuo su: accuratezza, anomalie, bias, conformità alla classificazione, evoluzione dei fornitori di modelli. Modifiche sostanziali comunicate con preavviso scritto di almeno trenta (30) giorni, salvo aggiornamenti correttivi/sicurezza. Le variazioni dei fornitori di modelli e delle relative garanzie sono comunicate e disciplinate ai sensi dell'Allegato G, §3.

9.3 Nuovi componenti. L'introduzione di ulteriori componenti algoritmici o AI è comunicata con le medesime modalità del §9.2 e con aggiornamento dell'inventario di cui ai §§6.1–6.2, mediante nuova versione del presente Allegato ex §10.3.

SEZIONE IV — DISPOSIZIONI COMUNI

10. Cooperazione regolamentare generale

10.1 Evoluzione normativa. Le Parti riconoscono che il quadro normativo in materia di NIS2, DORA e AI Act è in evoluzione. TimeFlow si impegna a monitorare gli sviluppi normativi rilevanti per i Servizi erogati e a cooperare in buona fede con la Committente per l'adeguamento delle misure contrattuali e tecniche, ove necessario.

10.2 Costi di adeguamento. Gli eventuali costi sostenuti da TimeFlow per adeguamenti tecnici o organizzativi resi necessari dall'evoluzione normativa sono gestiti secondo le disposizioni del MSA §18.3 (adeguamenti legali). Qualora tali adeguamenti impongano alla Committente oneri diretti e non marginali, si applica la procedura di negoziazione in buona fede prevista dal MSA §18.3.

10.3 Aggiornamento dell'Allegato. TimeFlow aggiorna il presente Allegato con cadenza almeno annuale, in corrispondenza di significative evoluzioni normative ovvero in occasione dell'introduzione di nuovi componenti algoritmici o di intelligenza artificiale nella Piattaforma, con preavviso scritto di almeno trenta (30) giorni ai sensi del MSA §18.3.

11. Prevalenza e disposizioni finali

11.1 Prevalenza. Si applica l'ordine di prevalenza tra i documenti contrattuali stabilito nel MSA §18.5. In caso di conflitto tra il presente Allegato e gli Allegati tecnici (C, D, F, G, K), prevale il presente Allegato limitatamente ai profili di compliance regolamentare.

11.2 Salvaguardia. L'eventuale invalidità o inapplicabilità di una o più disposizioni del presente Allegato non pregiudica la validità delle restanti disposizioni. Le Parti si impegnano a sostituire la disposizione invalida con una disposizione valida che persegua, nella misura più ampia possibile, la medesima finalità economica e giuridica.

11.3 Nessun aggravio sproporzionato. Nessuna disposizione del presente Allegato può essere interpretata nel senso di imporre a TimeFlow obblighi più gravosi di quelli ragionevolmente necessari per supportare la Committente nell'adempimento dei propri obblighi regolamentari. Ogni obbligo di cooperazione è reso nei limiti di quanto attinente ai Servizi erogati e proporzionato alla natura, alla scala e alla complessità dei medesimi.