ACCORDO DI CERTIFICAZIONE ORGANIZZATIVA CPF

PARTI

Il presente Accordo di Certificazione Organizzativa ("Accordo") è stipulato in data ___ del mese di _____, 20___ ("Data di Efficacia"), tra:

[**NOME ORGANISMO DI CERTIFICAZIONE**] ("Organismo di Certificazione" o "OdC")
Una [tipo di entità] di [giurisdizione]
Organismo di Certificazione CPF Autorizzato
Sede Principale: [Indirizzo]
Email: [Email]

E

[**NOME ORGANIZZAZIONE**] ("Organizzazione" o "Organizzazione Certificata" al momento della certificazione)
Una [tipo di entità] di [giurisdizione]
Numero di Registrazione: [Numero]
Sede Principale: [Indirizzo]
Email: [Email]

Collettivamente denominati le "Parti" e individualmente una "Parte."

PREMESSE

CONSIDERATO CHE, l'Organismo di Certificazione è autorizzato da CPF3 a gestire lo Schema di Certificazione CPF e certificare organizzazioni per la maturità nella gestione delle vulnerabilità psicologiche;

CONSIDERATO CHE, l'Organizzazione desidera ottenere la certificazione organizzativa secondo lo Schema di Certificazione CPF a uno dei quattro livelli di conformità (Livello 1-4);

CONSIDERATO CHE, l'Organizzazione ha implementato o sta implementando la metodologia CPF e i requisiti CPF-27001:2025;

CONSIDERATO CHE, l'Organismo di Certificazione è disposto a valutare l'implementazione dell'Organizzazione e concedere la certificazione se i requisiti sono soddisfatti;

PERTANTO, in considerazione dei reciproci impegni e accordi qui contenuti, le Parti convengono quanto segue:

1 DEFINIZIONI

1.1 "Certificazione" indica l'attestazione formale da parte dell'Organismo di Certificazione che l'Organizzazione ha raggiunto uno dei seguenti Livelli di Conformità CPF:

- Livello 1: Foundation (Punteggio CPF 100-149)
- Livello 2: Intermediate (Punteggio CPF 70-99)
- Livello 3: Advanced (Punteggio CPF 40-69)
- Livello 4: Exemplary (Punteggio CPF 0-39)

1.2 "Punteggio CPF" indica il punteggio aggregato di vulnerabilità (range 0-200) dove punteggi inferiori indicano una migliore postura di sicurezza.

1.3 "Ambito di Certificazione" indica le unità organizzative, le sedi e il personale coperti dalla certificazione, come dettagliato nell'Allegato A.

1.4 "CPF-27001:2025" indica lo standard dei requisiti del sistema di gestione CPF.

1.5 "Audit di Sorveglianza" indica l'audit periodico per verificare la conformità continuativa.

1.6 "Non Conformità" indica il mancato soddisfacimento di un requisito.

2 AMBITO E LIVELLO DI CERTIFICAZIONE

2.1 Ambito di Certificazione. La certificazione copre:

Entità Legale: _____

Unità Operative: _____

Sedi: _____

Personale Totale nell'Ambito: _____

Esclusioni: _____

Ambito dettagliato nell'Allegato A.

2.2 Livello di Certificazione Target:

☐ **Livello 1: Foundation** (Punteggio CPF 100-149)

☐ **Livello 2: Intermediate** (Punteggio CPF 70-99)

☐ **Livello 3: Advanced** (Punteggio CPF 40-69)

☐ **Livello 4: Exemplary** (Punteggio CPF 0-39)

3 PROCESSO DI CERTIFICAZIONE

3.1 Fase di Domanda. L'Organizzazione deve presentare:

- Modulo di domanda compilato
- Report di assessment CPF valido da Assessor/Auditor certificato
- Policy CPF approvata dall'alta direzione
- Organigramma che mostra i ruoli CPF
- Procedure di protezione della privacy
- Piani di trattamento dei rischi per indicatori Red
- Evidenza dell'integrazione ISMS
- Lettera di impegno della direzione
- Pagamento della tariffa di domanda

3.2 Revisione della Domanda. Entro 15 giorni lavorativi, l'Organismo di Certificazione deve:

- Verificare la completezza
- Verificare il Punteggio CPF e la validità dell'assessment
- Rivedere la documentazione per la conformità al livello target
- Approvare per l'audit o richiedere informazioni aggiuntive
- Assegnare un Auditor CPF qualificato

3.3 Audit di Certificazione.

Fase 1 (Revisione Documentale, 1-3 giorni):

- Revisione delle policy e procedure CPF
- Valutazione della prontezza per la Fase 2
- Identificazione delle lacune che richiedono correzione

Fase 2 (Revisione dell'Implementazione, 3-10 giorni):

- Verifica del Punteggio CPF attraverso campionamento
- Revisione della metodologia e protezioni della privacy
- Verifica del trattamento dei rischi
- Interviste con direzione e personale
- Revisione delle evidenze per i requisiti del livello target

- Valutazione dell'integrazione ISMS
- Valutazione dell'efficacia

Reportistica dell'Audit (15 giorni lavorativi):

- Riunioni di apertura e chiusura
- Report di audit scritto
- Risultati: NC Maggiore, NC Minore, Osservazione, Opportunità

3.4 Azioni Correttive. Se non conformità:

- L'Organizzazione presenta il piano entro 30 giorni
- NC maggiori corrette prima della certificazione
- NC minori correggibili entro 90 giorni dopo
- Verifica dell'efficacia

3.5 Decisione di Certificazione. Entro 15 giorni lavorativi:

- Concedere al livello appropriato
- Emettere il certificato e autorizzare l'uso del Marchio
- Aggiungere al registro pubblico
- Stabilire il programma di sorveglianza
- Oppure negare con spiegazione e diritti di appello

4 CONCESSIONE DELLA CERTIFICAZIONE E DIRITTI

4.1 Concessione della Certificazione:

- Certificazione del Livello di Conformità CPF
- Diritto di utilizzare il Marchio di Certificazione
- Inserimento nel registro pubblico
- Certificato valido 3 anni
- Accesso alle risorse

4.2 Uso del Marchio di Certificazione:

- Sito web e materiali marketing
- Proposte e presentazioni

- Sedi degli uffici
- Firme email
- Social media
- Indicare: "Organizzazione Certificata CPF - Livello [X]"

4.3 Restrizioni:

- Nessuna modifica al Marchio
- Non su prodotti/servizi (si applica all'organizzazione)
- Non per livello superiore a quello certificato
- Non al di fuori dell'ambito di certificazione
- Non dopo scadenza/sospensione/revoca
- Nessun trasferimento o sublicenza
- Nessuna dichiarazione fuorviante

5 OBBLIGHI

5.1 Mantenimento:

- Mantenere la gestione sistematica delle vulnerabilità
- Continuare l'implementazione CPF-27001:2025
- Mantenere/migliorare il Punteggio CPF entro il livello
- Aggiornare i trattamenti dei rischi
- Mantenere le pratiche di preservazione della privacy
- Fornire risorse adeguate

5.2 Personale:

- Mantenere il Coordinatore CPF
- Livello 2+: Minimo 1 Assessor certificato
- Livello 3+: Minimo 2 Assessor certificati
- Livello 4: Team dedicato con Auditor
- Assicurare il mantenimento CPE
- Fornire formazione di consapevolezza

5.3 Assessment e Monitoraggio:

- Livello 1: Assessment annuale
- Livello 2: Cicli trimestrali
- Livello 3+: Monitoraggio continuo
- Utilizzare professionisti certificati
- Mantenere la documentazione
- Tracciare le tendenze
- Riportare gli indicatori Red secondo i requisiti del livello

5.4 Riesame della Direzione:

- Livello 1: Annuale
- Livello 2: Semestrale
- Livello 3+: Trimestrale
- Documentare i riesami con metriche, decisioni, azioni

5.5 Riduzione degli Incidenti:

- Tracciare gli incidenti legati al fattore umano
- Stabilire la baseline
- Livello 2: 20% di riduzione
- Livello 3: 40% di riduzione
- Livello 4: 60% di riduzione
- Documentare le evidenze

5.6 Privacy ed Etica:

- Framework di protezione della privacy
- Mai utilizzare per profilazione individuale
- Aggregazione minima (10 individui)
- Livello 3+: Differential privacy ($\varepsilon \leq 0.1$)
- Reportistica con ritardo temporale (72 ore)
- Archiviazione e trasmissione sicure
- Livello 3-4: Audit privacy esterno annuale

5.7 Modifiche all'Ambito. Notificare entro 30 giorni:

- Cambiamenti organizzativi

- Espansioni/riduzioni dell'ambito
- Cambiamenti del personale (¿20%)
- Cambiamenti del Coordinatore CPF
- Qualsiasi cosa impatti la certificazione

5.8 Cooperazione:

- Concedere accesso per la sorveglianza
- Rispondere tempestivamente alle richieste
- Notificare immediatamente: violazioni, aumenti del punteggio, reclami, azioni legali, perdita di personale
- Implementare le azioni correttive

6 SORVEGLIANZA

6.1 Requisiti per Livello:

Livello 1:

- Sorveglianza annuale da Assessor (1-2 giorni)
- Revisione del programma e dei risultati

Livello 2:

- Biennale da Auditor (2-3 giorni)
- Revisione documentale trimestrale
- Verificare la riduzione degli incidenti

Livello 3:

- Annuale da Auditor (3-5 giorni)
- Revisione documentale trimestrale del monitoraggio
- Verifica annuale dell'audit privacy

Livello 4:

- Annuale da Auditor esterno (5-7 giorni)
- Revisione documentale mensile
- Audit privacy esterno trimestrale

- Peer review biennale

6.2 Processo:

- Preavviso di 30 giorni
- Focus: Tendenze del punteggio, metodologia, privacy, riesame della direzione, incidenti, modifiche
- Risultati documentati
- Azioni correttive per le NC

6.3 Risultati:

- Nessuna NC: Continuare
- NC minori: Piano entro 30 giorni, implementare entro 90
- NC maggiori: Azione immediata, sospensione se non corrette in 90 giorni

6.4 Monitoraggio del Punteggio CPF:

- Miglioramento: Può richiedere upgrade
- Degradazione fuori range: 90 giorni per ripristinare o downgrade
- Punteggio ¿149: Sospensione in attesa di azione correttiva

7 RICERTIFICAZIONE

7.1 Requisito. Ogni 3 anni.

7.2 Processo:

- Notifica 180 giorni prima della scadenza
- Domanda 120 giorni prima
- Audit di ricertificazione completo
- Assessment completo del Punteggio CPF
- Revisione delle tendenze triennali
- Valutazione del miglioramento continuo
- Audit minimo 60 giorni prima della scadenza
- Decisione entro 30 giorni
- Nuovo certificato con date aggiornate
- Il livello può cambiare in base al punteggio attuale

7.3 Tempistiche:

- Anticipata: Fino a 6 mesi prima (nuovo periodo dalla data effettiva)
- Ritardata: Ricertificazione completa come nuovo richiedente
- Nessun periodo di grazia

8 TARIFFE

8.1 Tariffa di Domanda:

1-50 dipendenti	$500
51-250	$1.000
251-1000	$1.500
1000+	$2.000

Non rimborsabile.

8.2 Tariffe di Audit:

Dimensione	Fase 1	Fase 2
1-50	$2.000	$4.000
51-250	$3.000	$7.000
251-1000	$5.000	$12.000
1000+	$8.000	$20.000

Complesso/multi-sito: $1.500/giorno aggiuntivo

8.3 Tariffa di Certificazione:

1-50	$1.000
51-250	$2.000
251-1000	$3.500
1000+	$5.000

8.4 Sorveglianza Annuale:

Livello 1	30% dell'audit iniziale
Livello 2	40% (biennale)
Livello 3	50%
Livello 4	60%

8.5 Ricertificazione:

- Audit: 75% dell'iniziale
- Tariffa: Stessa dell'iniziale

8.6 Altro:

- Espansione ambito: $1.000-$5.000
- Follow-up per NC maggiori: $1.500/giorno

- Upgrade di livello: $2.000-$8.000
- Urgente: 25% sovrapprezzo
- Viaggio: Costi effettivi

8.7 Pagamento:

- Domanda: Con presentazione
- Fase 1: Prima dell'audit
- Fase 2: Prima dell'audit
- Certificazione: Alla decisione
- Sorveglianza: 30 giorni prima
- Tutte le tariffe in USD
- Ritardo: 1,5% interesse mensile
- Servizi sospesi se ¿60 giorni di ritardo

9 SOSPENSIONE E REVOCA

9.1 Motivi di Sospensione:

- Punteggio fuori range
- NC maggiore non corretta (90 giorni)
- Mancato completamento della sorveglianza
- Mancato pagamento delle tariffe
- Violazione della privacy
- Perdita di personale chiave
- Cambiamenti organizzativi maggiori
- Uso improprio del Marchio

9.2 Processo di Sospensione:

- Notifica scritta con motivazioni
- Restrizione immediata sul nuovo uso del Marchio
- Registro: "Sospeso"
- Usi esistenti: Aggiungere "Certificazione Sospesa"
- Max 180 giorni

- Piano di risoluzione (30 giorni)
- Potrebbe essere richiesto audit di verifica
- Reintegro alla risoluzione
- Revoca se non risolto

9.3 Motivi di Revoca:

- Mancata risoluzione (180 giorni)
- Violazioni gravi della privacy
- Frode/dichiarazioni false/falsificazione
- Violazioni sistematiche di CPF-27001
- Profilazione individuale
- Violazione sostanziale
- Uso improprio persistente del Marchio
- Rifiuto di cooperare
- Insolvenza/fallimento

9.4 Processo di Revoca:

- Notifica scritta con motivazioni
- 30 giorni per rispondere
- Revisione da comitato indipendente
- Decisione entro 45 giorni
- Se revocato: Cessazione immediata, rimozione dal registro, avviso pubblico, restituzione certificato, nessun rimborso, divieto di riapplicazione per 2 anni
- Diritto di appello

9.5 Recesso Volontario:

- Preavviso 30 giorni
- Cessazione immediata
- Restituzione certificato
- Nessun rimborso
- Può riapplicare in qualsiasi momento

10 APPELLI

10.1 Diritto di Appello:

- Diniego di certificazione
- Determinazione del livello
- Sospensione
- Revoca
- Downgrade
- Dispute su NC maggiori

10.2 Processo:

- Scritto entro 30 giorni
- Tariffa: $500
- Motivazioni e prove
- Pannello indipendente
- Decisione entro 45 giorni
- Opzioni: Conferma/Modifica/Ribalta/Rimanda
- Tariffa rimborsata se con successo
- Finale e vincolante

11 RISERVATEZZA

11.1 Riservatezza dell'OdC:

- Mantenere la riservatezza di: Dati di assessment, punteggi, documenti interni, informazioni aziendali, metodi di privacy, risultati
- Limitare l'accesso al team di audit
- Non divulgare eccetto: Info del registro pubblico, a CPF3, a organismi di accreditamento, come richiesto dalla legge
- Il personale firma accordi di riservatezza

11.2 Protezione dei Dati:

- Conformità GDPR/CCPA
- Implementare misure di sicurezza

- Elaborare solo per la certificazione
- Notificare le violazioni (24 ore)
- Cooperare nella risposta alle violazioni

11.3 Conservazione:

- Registri: 7 anni dopo scadenza/revoca
- Report di audit: 7 anni
- Appelli/reclami: 10 anni
- Distruzione sicura

12 LIMITAZIONE DI RESPONSABILITÀ

12.1 Esclusione. NESSUNA GARANZIA RIGUARDO A RISULTATI AZIENDALI, PREVENZIONE INCIDENTI, CONFORMITÀ NORMATIVA O MIGLIORAMENTI ASSICURATIVI.

12.2 Limitazione. NESSUNA RESPONSABILITÀ PER DANNI INDIRETTI, CONSEQUENZIALI, SPECIALI O PUNITIVI.

12.3 Tetto. RESPONSABILITÀ TOTALE NON OLTRE LE TARIFFE PAGATE NEI 12 MESI PRECEDENTI IL RECLAMO.

12.4 Eccezioni: Negligenza grave, violazioni di riservatezza, violazioni della protezione dati, reclami non limitabili per legge.

13 INDENNIZZO

13.1 Dall'Organizzazione: Da reclami derivanti da uso improprio del Marchio, dichiarazioni false, violazioni della privacy, informazioni false, reclami di terze parti.

13.2 Dall'OdC: Da violazione di riservatezza, negligenza nell'audit, violazioni dei dati.

14 DISPOSIZIONI GENERALI

14.1 Legge Applicabile. [Giurisdizione]

14.2 Controversie. Negoziazione, mediazione, poi arbitrato.

14.3 Intero Accordo. Questo Accordo e Allegati.

14.4 Modifica. L'OdC può modificare CPF-27001 (180 giorni di preavviso).

14.5 Cessione. L'Organizzazione non può cedere; l'OdC può per trasferimento aziendale.

14.6 Forza Maggiore. Nessuno responsabile per eventi oltre il controllo.

14.7 Notifiche. Scritte agli indirizzi indicati.

14.8 Separabilità. Disposizioni non valide riformate.

14.9 Sopravvivenza. Sezioni 10, 12, 13, 14 sopravvivono.

FIRME

ORGANISMO DI CERTIFICAZIONE:

Per: _____ Data: _____

Nome: _____ Titolo: _____

ORGANIZZAZIONE:

Per: _____ Data: _____

Nome: _____ Titolo: _____

ALLEGATO A: AMBITO DI CERTIFICAZIONE

Entità Legale: _____

Unità Operative: _____

Sedi: _____

Personale Totale: _____

Esclusioni: _____

Giustificazione: _____

Approvato da:

OdC: _____ Data: _____

Org: _____ Data: _____