

# MOP - Manuale Operativo Privacy

## 1. Introduzione

### 1.1 Scopo del Manuale

Il presente Manuale Operativo Privacy (MOP) è stato redatto per fornire una guida dettagliata sulle politiche, le procedure e le misure adottate da CFLC - Cooperativa Formazione Lavoro Cooperazione - Impresa Sociale, per garantire la protezione dei dati personali trattati dall'azienda. Il manuale è finalizzato a garantire la conformità alle normative vigenti in materia di protezione dei dati, in particolare al Regolamento (UE) 2016/679 (GDPR).

### 1.2 Ambito di Applicazione

Il MOP si applica a tutte le attività di trattamento dei dati personali svolte da CFLC, includendo ma non limitandosi a, la gestione del personale, l'erogazione di servizi di formazione, l'orientamento e avviamento al lavoro, la gestione dei rapporti con i fornitori, le attività di marketing e comunicazione, la gestione dei servizi di supporto agli utenti, la gestione dei sistemi informativi e l'adempimento degli obblighi legali e normativi. Il manuale è destinato a tutti i dipendenti, collaboratori e partner che operano sotto l'autorità di CFLC.

### 1.3 Definizioni e Terminologia

Per una corretta comprensione del MOP, si riportano di seguito alcune definizioni e termini chiave utilizzati nel documento:

- **Dati Personali:** Qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato).
- **Interessato:** La persona fisica alla quale si riferiscono i dati personali.
- **Trattamento:** Qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
- **Titolare del Trattamento:** La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
- **Responsabile del Trattamento:** La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
- **Responsabile della Protezione dei Dati (DPO):** La persona designata dal titolare o dal responsabile del trattamento per svolgere le funzioni di cui agli articoli 37-39 del GDPR.
- **Consenso:** Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso,

mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

- **Violazione dei Dati Personali:** La violazione della sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

---

## 2. Informazioni Generali

### 2.1 Dati del Titolare del Trattamento

- **Nome del Titolare del Trattamento:** CFLC - Cooperativa Formazione Lavoro Cooperazione - Impresa Sociale
- **Indirizzo:** Via Varese, 2/8, 16122 Genova
- **P.IVA:** [Inserire P.IVA]
- **Codice Fiscale:** [Inserire Codice Fiscale]
- **Numero di Iscrizione al Registro delle Imprese:** [Inserire Numero]
- **Rappresentante Legale:** [Nome del Rappresentante Legale]
- **Contatti:** [Inserire contatti: telefono, email]

---

## 3. Policy CFLC

### 3.1 Chi Siamo

CFLC - Cooperativa Formazione Lavoro Cooperazione - Impresa Sociale è una cooperativa sociale con sede a Genova, specializzata nella formazione professionale, nell'orientamento al lavoro e nella promozione dell'inclusione sociale. La nostra missione è fornire opportunità di crescita personale e professionale a individui di tutte le età, con particolare attenzione a coloro che si trovano in situazioni di svantaggio sociale ed economico.

### 3.2 Servizi Offerti

CFLC offre una vasta gamma di servizi per soddisfare le esigenze di formazione e inserimento lavorativo della comunità. I principali servizi includono:

- **Formazione Professionale:** Corsi di formazione in vari settori professionali, progettati per migliorare le competenze e aumentare l'occupabilità dei partecipanti.
- **Orientamento al Lavoro:** Programmi di orientamento e consulenza per aiutare le persone a identificare e perseguire le loro ambizioni professionali.
- **Inserimento Lavorativo:** Collaborazione con aziende partner per facilitare l'inserimento lavorativo dei nostri studenti e candidati.
- **Servizi di Supporto:** Assistenza personalizzata e servizi di supporto per aiutare i partecipanti a superare le difficoltà e a raggiungere i loro obiettivi formativi e lavorativi.

### 3.3 Politiche di Protezione dei Dati

CFLC adotta una serie di politiche e misure per garantire la protezione dei dati personali trattati nell'ambito delle sue attività. Le nostre politiche di protezione dei dati si basano sui seguenti principi fondamentali:

- **Legalità, Correttezza e Trasparenza:** I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti degli interessati.
- **Limitazione delle Finalità:** I dati personali sono raccolti per finalità determinate, esplicite e legittime e non sono ulteriormente trattati in modo incompatibile con tali finalità.
- **Minimizzazione dei Dati:** I dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
- **Esattezza:** I dati personali sono esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti.
- **Limitazione della Conservazione:** I dati personali sono conservati in una forma che consente l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.
- **Integrità e Riservatezza:** I dati personali sono trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione contro il trattamento non autorizzato o illecito e dalla perdita, distruzione o danno accidentale, mediante misure tecniche e organizzative adeguate.
- **Responsabilità:** Il titolare del trattamento è responsabile del rispetto dei principi sopra elencati e deve essere in grado di provarlo.

### 3.4 Impegno alla Conformità

CFLC si impegna a mantenere elevati standard di conformità alle normative sulla protezione dei dati personali, in particolare il Regolamento (UE) 2016/679 (GDPR). L'azienda si assicura che tutte le sue attività di trattamento dei dati siano svolte in conformità con le leggi e i regolamenti applicabili, adottando misure adeguate per proteggere i dati personali e garantire i diritti degli interessati.

---

## 4. Misure di Sicurezza

CFLC attribuisce grande importanza alla sicurezza dei dati personali e adotta un approccio proattivo nell'implementazione e nel mantenimento delle misure di sicurezza. La protezione dei dati personali è una priorità per garantire la fiducia dei nostri dipendenti, studenti, candidati e partner.

### 4.1 Misure di Sicurezza Organizzative

Le misure organizzative sono fondamentali per stabilire una cultura aziendale orientata alla sicurezza e alla protezione dei dati. CFLC implementa policy e procedure chiare, forma costantemente il personale e garantisce che tutte le persone coinvolte nel trattamento dei dati comprendano le loro responsabilità. Attraverso accordi di riservatezza, gestione rigorosa degli incidenti di sicurezza, audit periodici e una documentazione accurata delle attività di

trattamento, CFLC assicura che tutte le operazioni siano condotte in conformità con il GDPR. Queste misure organizzative sono regolarmente revisionate e aggiornate per adattarsi ai cambiamenti normativi e alle nuove minacce alla sicurezza.

#### **4.1.1 Policy di Accesso ai Dati**

CFLC implementa policy di accesso ai dati basate sul principio del "need-to-know". Solo il personale autorizzato, che necessita di accedere ai dati personali per svolgere le proprie mansioni, ha accesso ai dati. Le autorizzazioni di accesso sono definite chiaramente e vengono riesaminate periodicamente per garantire che siano adeguate alle responsabilità attuali dei dipendenti. La registrazione e il monitoraggio degli accessi ai dati sensibili sono effettuati per prevenire accessi non autorizzati e garantire la tracciabilità.

#### **4.1.2 Formazione del Personale**

La formazione del personale è una componente cruciale delle misure di sicurezza organizzative di CFLC. Tutti i nuovi assunti partecipano a programmi di formazione obbligatoria riguardanti le politiche aziendali sulla privacy e la protezione dei dati. Inoltre, CFLC organizza sessioni di aggiornamento periodiche per tutti i dipendenti, con particolare attenzione alle novità normative e ai nuovi rischi di sicurezza. La valutazione periodica delle conoscenze del personale attraverso test e simulazioni garantisce la consapevolezza e la comprensione delle procedure di sicurezza.

#### **4.1.3 Accordi di Riservatezza**

CFLC richiede a tutti i dipendenti e collaboratori di firmare accordi di riservatezza come parte integrante del contratto di lavoro. Questi accordi includono clausole specifiche per il trattamento dei dati sensibili e per la protezione delle informazioni aziendali riservate. Le procedure per l'aggiornamento e la revisione degli accordi di riservatezza sono attuate in caso di cambiamenti nelle responsabilità o nelle mansioni dei dipendenti.

#### **4.1.4 Procedure di Gestione degli Incidenti di Sicurezza**

CFLC ha definito procedure chiare e dettagliate per la gestione degli incidenti di sicurezza dei dati. Queste procedure includono un protocollo per la segnalazione immediata di incidenti di sicurezza da parte del personale e la creazione di un team di risposta agli incidenti (Incident Response Team). Il team è incaricato di analizzare, contenere e risolvere gli incidenti. Tutti gli incidenti sono documentati e analizzati per identificare le cause e implementare misure preventive. In caso di violazioni dei dati personali, CFLC comunica tempestivamente le violazioni alle autorità competenti e agli interessati, in conformità con il GDPR.

#### **4.1.5 Audit e Controlli Periodici**

CFLC realizza audit e controlli periodici per verificare la conformità alle normative sulla protezione dei dati. Gli audit interni valutano l'efficacia delle misure di sicurezza e delle procedure di protezione dei dati, mentre le verifiche esterne, condotte da auditor indipendenti, garantiscono l'oggettività e l'affidabilità delle valutazioni. Il monitoraggio continuo delle attività di trattamento dei dati consente di identificare e correggere eventuali non conformità.

#### **4.1.6 Documentazione delle Attività di Trattamento**

CFLC mantiene un registro dettagliato e aggiornato delle attività di trattamento dei dati personali. Il registro include tutte le attività di trattamento, comprese le finalità, le categorie di dati, i destinatari e i termini di conservazione. Il registro è aggiornato continuamente per riflettere eventuali modifiche nelle attività di trattamento ed è disponibile per le autorità competenti in caso di richiesta di verifica.

#### **4.1.7 Gestione dei Consensi**

CFLC implementa procedure per l'acquisizione, la gestione e la revoca dei consensi degli interessati. Il consenso è raccolto in modo chiaro e trasparente, con informazioni dettagliate sulle finalità del trattamento. I consensi ottenuti e le eventuali revoche sono registrati accuratamente. Le procedure per gestire le richieste di revoca del consenso garantiscono che i dati siano trattati solo in base ai consensi validi.

### **4.2 Misure di Sicurezza Tecniche**

Le misure tecniche sono essenziali per proteggere i dati personali da accessi non autorizzati, perdite e altre minacce. CFLC utilizza firewall, software antivirus, tecniche di crittografia e sistemi di controllo degli accessi per garantire la sicurezza delle informazioni trattate. Backup regolari dei dati, aggiornamenti tempestivi di software e patch di sicurezza, insieme a un monitoraggio costante e logging delle attività di sistema, sono implementati per prevenire e rispondere rapidamente a qualsiasi incidente di sicurezza. Inoltre, la protezione fisica delle infrastrutture informatiche è garantita attraverso misure come serrature, sistemi di allarme e controlli di accesso fisico. CFLC si impegna a rimanere aggiornata sulle migliori pratiche e tecnologie disponibili per migliorare continuamente la sicurezza dei dati.

#### **4.2.1 Firewall**

CFLC implementa firewall per proteggere la rete aziendale da accessi non autorizzati e attacchi informatici. I firewall sono configurati per monitorare e controllare il traffico in entrata e in uscita, garantendo che solo le comunicazioni autorizzate possano accedere alla rete interna. I firewall sono aggiornati regolarmente per mantenere un alto livello di protezione.

#### **4.2.2 Antivirus**

Tutti i dispositivi aziendali sono dotati di software antivirus per rilevare e rimuovere malware. Il software antivirus viene aggiornato regolarmente per garantire la protezione contro le minacce più recenti. CFLC esegue scansioni periodiche su tutti i dispositivi per identificare e neutralizzare eventuali minacce informatiche.

#### **4.2.3 Crittografia**

CFLC utilizza tecniche di crittografia per proteggere i dati sensibili durante la trasmissione e l'archiviazione. Le comunicazioni via email e altre forme di trasferimento dati sono protette tramite protocolli di crittografia avanzati. La crittografia garantisce che i dati siano accessibili solo a persone autorizzate e protegge le informazioni da accessi non autorizzati.

#### **4.2.4 Backup Regolari**

CFLC esegue backup regolari dei dati aziendali per prevenire la perdita di informazioni importanti. Le copie di backup sono conservate in luoghi sicuri e separati dal sistema principale per garantire la disponibilità dei dati in caso di incidenti. L'integrità delle copie di backup viene verificata periodicamente per assicurare la loro affidabilità.

#### **4.2.5 Controllo degli Accessi**

CFLC implementa sistemi di autenticazione forte per l'accesso ai sistemi informativi. L'autenticazione a due fattori (2FA) è utilizzata per aggiungere un ulteriore livello di sicurezza. Le credenziali di accesso sono gestite in modo sicuro e centralizzato. Gli accessi ai sistemi critici sono registrati e monitorati per rilevare attività sospette e garantire la tracciabilità.

#### **4.2.6 Aggiornamenti e Patch**

CFLC garantisce l'installazione tempestiva di aggiornamenti e patch di sicurezza per tutti i sistemi e software utilizzati. Il monitoraggio delle vulnerabilità consente di identificare rapidamente i punti deboli e di applicare le patch necessarie per mitigare i rischi. Gli aggiornamenti regolari migliorano la sicurezza complessiva del sistema.

#### **4.2.7 Monitoraggio e Logging**

CFLC implementa sistemi di monitoraggio per rilevare attività sospette e incidenti di sicurezza. I log degli eventi di sicurezza significativi e degli accessi ai sistemi sono configurati per garantire la completezza e l'inalterabilità. L'analisi periodica dei log consente di individuare potenziali minacce e di rispondere prontamente agli incidenti di sicurezza.

#### **4.2.8 Protezione Fisica**

CFLC adotta misure di sicurezza fisica per proteggere le infrastrutture informatiche. L'uso di serrature, sistemi di allarme e controllo degli accessi fisici garantisce che solo le persone autorizzate possano accedere ai locali in cui sono conservati i dati e i dispositivi. I dispositivi di archiviazione rimovibili e i supporti di backup sono conservati in luoghi sicuri per prevenire furti e danni.

### **5. Procedure Operative**

CFLC ha implementato una serie di procedure operative per garantire la corretta gestione dei dati personali e la conformità alle normative vigenti. Queste procedure sono progettate per assicurare che tutte le attività di trattamento dei dati siano condotte in modo sicuro, trasparente e rispettoso dei diritti degli interessati.

#### **5.1 Acquisizione e Gestione dei Consensi**

CFLC ha sviluppato procedure dettagliate per l'acquisizione e la gestione dei consensi degli interessati. Il consenso è raccolto in modo chiaro e trasparente, con informazioni dettagliate sulle finalità del trattamento. CFLC garantisce che il consenso sia libero, specifico, informato e inequivocabile. Le richieste di consenso includono tutte le informazioni necessarie per

permettere agli interessati di prendere decisioni consapevoli. I consensi ottenuti e le eventuali revoche sono registrati accuratamente, e CFLC gestisce le richieste di revoca del consenso per garantire che i dati siano trattati solo in base ai consensi validi.

## **5.2 Gestione delle Richieste degli Interessati**

CFLC ha implementato procedure per gestire le richieste degli interessati relative ai loro diritti in materia di protezione dei dati personali, come il diritto di accesso, rettifica, cancellazione, limitazione del trattamento, portabilità dei dati e opposizione. Le richieste sono gestite in modo tempestivo e trasparente, in conformità con i requisiti del GDPR. CFLC fornisce risposte alle richieste degli interessati entro un mese dal ricevimento della richiesta, salvo casi di particolare complessità. In tali casi, gli interessati sono informati della necessità di un'estensione del termine.

## **5.3 Procedure per la Segnalazione di Violazioni dei Dati**

CFLC ha definito procedure chiare per la segnalazione e la gestione delle violazioni dei dati personali. Queste procedure includono un protocollo per la segnalazione immediata di incidenti di sicurezza da parte del personale e la creazione di un team di risposta agli incidenti. Il team è incaricato di analizzare, contenere e risolvere gli incidenti, e di comunicare tempestivamente le violazioni alle autorità competenti e agli interessati, in conformità con il GDPR. Tutti gli incidenti sono documentati e analizzati per identificare le cause e implementare misure preventive.

## **5.4 Valutazione e Mitigazione dei Rischi**

CFLC effettua valutazioni periodiche dei rischi associati al trattamento dei dati personali. Queste valutazioni includono l'analisi delle potenziali minacce e vulnerabilità, e la determinazione delle misure di sicurezza necessarie per mitigare i rischi identificati. CFLC adotta un approccio proattivo alla gestione dei rischi, implementando misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio. Le valutazioni dei rischi sono riviste e aggiornate regolarmente per riflettere i cambiamenti nelle attività di trattamento e nelle minacce alla sicurezza.

# **6. Documentazione e Archiviazione**

CFLC riconosce l'importanza di mantenere una documentazione accurata e completa delle attività di trattamento dei dati personali. La corretta gestione e archiviazione dei documenti sono essenziali per garantire la trasparenza, la conformità e la protezione dei dati.

## **6.1 Registro delle Attività di Trattamento**

CFLC mantiene un registro dettagliato delle attività di trattamento dei dati personali, come richiesto dall'articolo 30 del GDPR. Questo registro include informazioni sulle finalità del trattamento, le categorie di dati trattati, le categorie di interessati, le categorie di destinatari dei dati, i termini di conservazione e le misure di sicurezza applicate. Il registro è aggiornato regolarmente per riflettere eventuali modifiche nelle attività di trattamento.

## **6.2 Moduli e Form di Consenso**

CFLC utilizza moduli e form di consenso standardizzati per raccogliere e documentare il consenso degli interessati al trattamento dei loro dati personali. Questi documenti includono informazioni dettagliate sulle finalità del trattamento, le basi giuridiche e i diritti degli interessati. I consensi ottenuti sono registrati e conservati in modo sicuro, e le richieste di revoca del consenso sono gestite tempestivamente.

### **6.3 Contratti e Accordi di Riservatezza**

Tutti i contratti con dipendenti, collaboratori e fornitori includono clausole specifiche relative alla protezione dei dati personali e alla riservatezza. CFLC assicura che tutti i soggetti coinvolti nel trattamento dei dati personali siano a conoscenza delle loro responsabilità e abbiano firmato accordi di riservatezza appropriati. Questi documenti sono conservati e aggiornati periodicamente.

### **6.4 Rapporti di Audit e Controllo**

CFLC realizza audit interni ed esterni per verificare la conformità alle normative sulla protezione dei dati e l'efficacia delle misure di sicurezza implementate. I risultati degli audit sono documentati in rapporti dettagliati, che includono le eventuali non conformità riscontrate e le azioni correttive intraprese. Questi rapporti sono conservati per future consultazioni e revisioni.

### **6.5 Registro degli Incidenti di Sicurezza**

CFLC mantiene un registro degli incidenti di sicurezza che include tutte le violazioni dei dati personali, le misure adottate per risolvere gli incidenti e le comunicazioni inviate alle autorità competenti e agli interessati. Questo registro è aggiornato tempestivamente e analizzato periodicamente per identificare tendenze e migliorare le misure di sicurezza.

### **6.6 Conservazione e Distruzione dei Documenti**

CFLC adotta politiche chiare per la conservazione e la distruzione dei documenti contenenti dati personali. I documenti sono conservati per il periodo necessario a conseguire le finalità per le quali sono stati raccolti, in conformità con i termini di conservazione stabiliti. Alla scadenza del periodo di conservazione, i documenti sono distrutti in modo sicuro per prevenire accessi non autorizzati e proteggere la riservatezza dei dati.

## **7. Ruoli e Responsabilità**

CFLC definisce chiaramente i ruoli e le responsabilità all'interno dell'organizzazione per garantire una gestione efficace della protezione dei dati personali. Ogni ruolo ha compiti specifici che contribuiscono alla sicurezza e alla conformità con il GDPR.

### **7.1 Titolare del Trattamento**

Il Titolare del Trattamento è la persona fisica o giuridica che determina le finalità e i mezzi del trattamento dei dati personali. In particolare:

- Garantire la conformità alle normative sulla protezione dei dati.
- Stabilire politiche e procedure per la protezione dei dati.



- Assicurare che siano adottate adeguate misure tecniche e organizzative.
- Valutare e mitigare i rischi associati al trattamento dei dati personali.
- Designare un Responsabile della Protezione dei Dati (DPO), se richiesto.

## **7.2 Amministratori di Sistema**

Gli Amministratori di Sistema sono responsabili della gestione tecnica dei sistemi informativi che trattano dati personali. In particolare:

- Garantire la sicurezza e la protezione dei sistemi informativi.
- Implementare e mantenere misure di sicurezza tecniche, come firewall, antivirus e backup.
- Monitorare gli accessi ai sistemi e prevenire accessi non autorizzati.
- Assicurare l'aggiornamento e la manutenzione regolare dei sistemi.
- Documentare e segnalare eventuali incidenti di sicurezza.

## **7.3 Responsabili del Trattamento**

I Responsabili del Trattamento sono terze parti che trattano dati personali per conto del Titolare del Trattamento. In particolare:

- Trattare i dati personali esclusivamente per le finalità definite dal Titolare del Trattamento.
- Implementare misure tecniche e organizzative adeguate per proteggere i dati personali.
- Informare immediatamente il Titolare del Trattamento in caso di violazioni dei dati.
- Garantire la formazione e la sensibilizzazione del proprio personale in materia di protezione dei dati.

## **7.4 Dipendenti e Collaboratori**

Tutti i dipendenti e collaboratori che trattano dati personali nell'ambito delle loro mansioni. In particolare:

- Rispettare le politiche e le procedure aziendali in materia di protezione dei dati.
- Trattare i dati personali in modo sicuro e conforme alle normative.
- Segnalare tempestivamente eventuali incidenti di sicurezza o violazioni dei dati.
- Partecipare alle sessioni di formazione e sensibilizzazione organizzate dall'azienda.

# **8. Formazione e Sensibilizzazione**

CFLC riconosce l'importanza della formazione e della sensibilizzazione del personale in materia di protezione dei dati personali. Una corretta formazione e una costante sensibilizzazione sono fondamentali per garantire che tutti i dipendenti e collaboratori comprendano le loro responsabilità e le migliori prassi per la gestione sicura dei dati.

## **8.1 Programmi di Formazione**

CFLC organizza programmi di formazione obbligatoria per tutti i nuovi assunti e corsi di aggiornamento periodici per tutti i dipendenti e collaboratori. In particolare:

- I programmi di formazione iniziale coprono le politiche aziendali sulla privacy, le normative vigenti in materia di protezione dei dati (incluso il GDPR) e le procedure interne per la gestione sicura dei dati personali.
- I corsi di aggiornamento periodici affrontano le novità normative, i nuovi rischi di sicurezza e le migliori prassi per la protezione dei dati.
- La formazione è progettata per essere interattiva e coinvolgente, con esempi pratici e casi di studio per facilitare l'apprendimento.

## **8.2 Aggiornamenti Periodici**

CFLC si impegna a fornire aggiornamenti periodici sulle normative in materia di protezione dei dati e sulle migliori prassi per la sicurezza informatica. In particolare:

- Newsletter e comunicazioni interne per informare il personale su eventuali cambiamenti normativi e nuove procedure.
- Workshop e seminari periodici per approfondire temi specifici e promuovere la cultura della sicurezza.
- Accesso continuo a risorse formative online per permettere al personale di rimanere aggiornato in qualsiasi momento.

## **9. Revisione e Aggiornamento del MOP**

CFLC riconosce l'importanza di mantenere il Manuale Operativo Privacy (MOP) aggiornato e conforme alle normative vigenti in materia di protezione dei dati personali. La revisione periodica e l'aggiornamento del MOP garantiscono che le politiche e le procedure di protezione dei dati riflettano le best practice e le evoluzioni normative.

### **9.1 Frequenza delle Revisioni**

Il MOP è soggetto a revisioni periodiche per garantirne l'adeguatezza e la conformità. In particolare:

- Il MOP viene rivisto almeno una volta all'anno.
- Ulteriori revisioni possono essere effettuate in risposta a cambiamenti normativi, evoluzioni tecnologiche o incidenti di sicurezza.

### **9.2 Procedure di Aggiornamento**

Le procedure per l'aggiornamento del MOP sono chiaramente definite e includono i seguenti passaggi:

- Identificazione delle aree che richiedono aggiornamenti basati su nuove normative, cambiamenti organizzativi o risultati di audit.
- Consultazione con i responsabili dei vari dipartimenti per raccogliere input e suggerimenti.
- Redazione delle modifiche e integrazioni necessarie.
- Revisione delle modifiche da parte del Titolare del Trattamento e, se applicabile, degli Amministratori di Sistema.
- Approvazione finale e adozione delle modifiche.

### **9.3 Comunicazione delle Modifiche**

Una volta approvate, le modifiche al MOP vengono comunicate tempestivamente a tutti i dipendenti e collaboratori. In particolare:

- Le modifiche sono documentate e distribuite tramite comunicazioni interne, come email o intranet aziendale.
- Sessioni di formazione e sensibilizzazione sono organizzate per assicurare che tutto il personale comprenda le modifiche apportate e le nuove procedure da seguire.

### **9.4 Documentazione delle Revisioni**

CFLC mantiene un registro dettagliato di tutte le revisioni e aggiornamenti del MOP. In particolare:

- Ogni revisione è documentata con la data, la descrizione delle modifiche apportate e i motivi della revisione.
- Il registro delle revisioni è conservato per garantire la trasparenza e fornire un riferimento storico delle modifiche effettuate.

## **DOCUMENTAZIONE ALLEGATA**

### **Documenti GDPR**

- DOC\_01 - Privacy Policy
- DOC\_02 - Registro Attività di Trattamento Titolare
- DOC\_03 - Nomina Responsabili del Trattamento
- DOC\_04 - Nomina Autorizzati al Trattamento

### **Procedure**

- PRO\_01 - Procedura Gestione Incidenti
- PRO\_02 - Procedura Gestione Consensi
- PRO\_03 - Procedura Gestione Diritti Interessati
- PRO\_04 - Procedura Conservazione e Distruzione Documenti